



UNIVERSIDAD
POLITECNICA
DE VALENCIA



Escola Tècnica
Superior d'Enginyeria
Informàtica

UNIVERSIDAD POLITÉCNICA DE VALENCIA
ESCUELA TÉCNICA SUPERIOR DE INGENIERÍA INFORMÁTICA

Aproximación Ética y Legal a las Redes Sociales

Proyecto Fin de Carrera

Septiembre 2010

Autor: Pedro David Martín Mompó

Director: Juan Vicente Oltra Gutiérrez

Índice

Índice	2
1. Introducción. Objetivos del PFC.	4
2. Las redes sociales	6
a. Definición	6
b. Historia	8
c. Tipos y clasificación de las redes sociales	10
d. El impacto de las redes sociales en la sociedad	13
i. Todo un éxito entre los más jóvenes	13
ii. Una nueva forma de relacionarse	14
iii. Un nuevo poder mediático.....	15
e. Las redes sociales más utilizadas	18
i. Facebook	18
ii. Tuenti	20
iii. Twitter	22
3. Aspectos legales de la informática.....	24
a. Marco general	24
i. Convenios internacionales	24
ii. Legislación europea.....	29
iii. Legislación española.....	31
b. Contrato de adhesión.....	44
i. Facebook	44
ii. Tuenti	49
iii. Twitter	51
c. Derechos potencialmente vulnerables	53
i. Derecho al Honor	53
ii. Intimidad Personal y Familiar.....	53
iii. Derecho a la propia imagen	54
iv. Derecho a la libertad	54
v. Libertad de expresión.....	55
vi. Propiedad intelectual	55
vii. Propiedad industrial	56
d. Sanciones.....	57
i. Delitos contra el honor.....	57

ii.	Delitos contra la libertad	58
iii.	Delitos contra la propiedad intelectual e industrial.....	58
iv.	Delitos relacionados con la protección de datos personales.....	59
e.	Delitos informáticos típicos de las redes sociales	59
i.	Acceso a información confidencial.....	59
ii.	Suplantación de identidad	59
iii.	Creación de perfiles falsos	61
iv.	Fraude informático.....	61
v.	Daño o sabotaje informático.....	61
4.	Aplicaciones de las redes sociales	62
a.	Las redes sociales y la empresa	62
i.	Uso interno en las empresas	62
ii.	Uso externo en las empresas	63
b.	Las redes sociales y la política	66
c.	Uso en la docencia	73
i.	Motivación	73
ii.	Ventajas.....	74
iii.	Plataformas	75
5.	Peligros de las redes sociales	78
a.	Publicación de datos sensibles.....	78
i.	Vida sexual y amorosa.....	78
ii.	Vida privada.....	78
b.	Peligros para los menores	85
i.	Pornografía infantil	85
ii.	Ciberbullying.....	86
iii.	Apología de la anorexia y la bulimia.....	89
c.	Análisis de redes sociales	91
i.	Teoría de redes sociales	91
ii.	Peligro para la privacidad.....	91
6.	Conclusiones.....	94
REFERENCIAS.....		97
Otro material consultado		103

1.Introducción. Objetivos del PFC.

En los últimos años, hemos sido testigos del tremendo auge de las redes sociales en Internet. Hasta hace relativamente poco era un fenómeno apenas conocido, pero ha pasado a convertirse en un elemento importante en la vida de muchas personas. Y es que hoy día las redes sociales suponen mucho más que escribir mensajes o subir contenidos: suponen una nueva forma de relacionarse sin necesidad de salir de casa, con conocidos o desconocidos. También han revolucionado la forma de hacer negocios, de buscar trabajo, de hacer política, y hasta de enseñar. Como veremos, las aplicaciones prácticas son numerosas y muchas pueden repercutir de manera beneficiosa para la sociedad.

En realidad, la creación de este tipo de páginas no son más que el fruto de una evolución natural de Internet. Hemos pasado progresivamente de la Web 1.0, estática y sin interacción, a un entorno completamente interactivo, en el que los usuarios pueden compartir todo tipo de información en tiempo real con el resto del mundo. Por una parte, los adelantos técnicos han favorecido su aparición. El ancho de banda ha aumentado notablemente y los ordenadores se han convertido en potentes máquinas capaces de reproducir todo tipo de material multimedia. Paralelamente, han ido surgiendo nuevos lenguajes de programación que permiten la inserción de contenido dinámico. Pero lo más importante, es que hoy en día estamos casi todos *online*. Una red social en Internet sin usuarios no tendría ningún sentido.

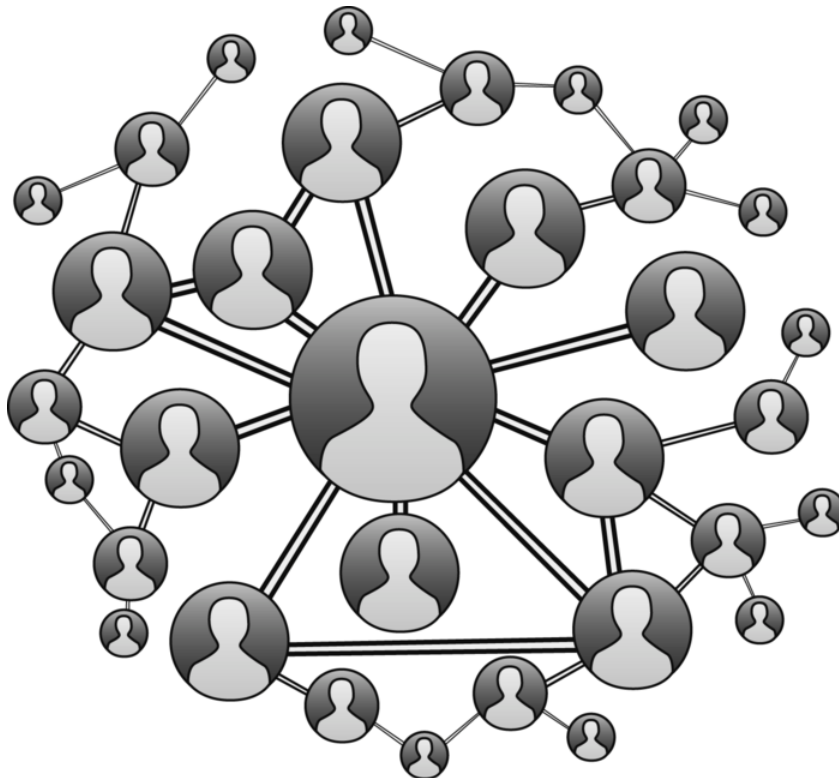
El concepto de “red social” no es ni mucho menos nuevo. Este término se lleva empleando durante más de un siglo para designar el complejo entramado de relaciones entre los miembros de diferentes sistemas sociales a todas las escalas, desde la personal hasta la internacional. Las redes sociales existen desde que el hombre vive en sociedad. La constituyen los familiares, amigos del colegio, vecinos, compañeros de trabajo... Ahora, esta red que siempre ha existido de una forma no tan evidente, se ha plasmado también en un plano virtual, de una forma esquemática y visible para el propio individuo y para los demás.

A pesar de todas sus bondades, las redes sociales pueden hacer peligrar los derechos de los usuarios. Por este motivo, estudiaremos la legislación existente al respecto a varios niveles. En el caso de España, se tendrán que acatar tratados internacionales, directivas europeas y, por supuesto, la legislación española, perfectamente alineada con dichas directivas. Dentro del marco legal español, extraeremos las leyes susceptibles de entrar en conflicto con las redes sociales, esto es la Ley Orgánica de Protección de Datos (LOPD), la Ley de Servicios de la Sociedad de la Información y de Comercio Electrónico (LSSI) y por último la Ley de Propiedad Intelectual (LPI). Analizaremos al detalle los contratos de adhesión de distintas redes sociales prestando especial atención a que cumplan correctamente dichas legislaciones. Veremos que la mera utilización de una red social puede llevar a que se vulneren muchos derechos de los ciudadanos en nuestro país, algunos incluso a pesar de atenerse estrictamente a los términos establecidos en cada una de estas redes sociales.

Desgraciadamente, a menudo se hace uso de estas redes con fines oscuros. Estas facilitan la perpetración de gran cantidad de delitos informáticos con fines lucrativos, como el robo de información confidencial o el fraude, los cuales son difíciles de detectar, y muchas legislaciones nacionales todavía no prevén estos escenarios

debido a su novedad. También aportan información valiosa sobre la vida privada que motiva delitos más “tradicionales”, como el robo, el secuestro o las amenazas. Asimismo, se ha detectado un repunte de la pornografía infantil en relación con este tipo de páginas, así como una nueva dimensión del acoso escolar, los cuales también serán caso de estudio en este proyecto.

Por otra parte, las redes sociales son una herramienta poderosa para analizar, persuadir y mover a las masas. Ya sea para promocionar un nuevo producto o para convencer a cierto público para que vote un determinado partido, veremos que algunas prácticas pueden ser poco éticas o incluso ilegales. Ciertos grupos y empresas realizan análisis de conducta y de información a través de los contenidos publicados. La información es poder y las redes sociales son al fin y al cabo un enorme archivo de información personal de millones de personas. Afortunadamente las propias redes sociales poseen sus mecanismos de privacidad, y la tendencia actual es a proteger a los usuarios en la medida de lo posible.



2. Las redes sociales

a. Definición

Basadas en el concepto de los *seis grados de separación* (la idea de que dos personas cualesquiera en el mundo podrían entrar en contacto a través de no más de cinco intermediarios), las redes sociales establecen comunidades de Internet interconectadas que posibilitan establecer contactos interesantes que de otro modo no sería posible. A grandes rasgos, funcionan de la siguiente manera: tras el registro, el usuario invita a la gente que conoce. Estos invitan a su vez a sus contactos, y el proceso se repite para cada persona. En teoría, cada individuo puede relacionarse con alguien a través de otro usuario con quien ya se está relacionado.

Definiremos las redes sociales en Internet como los servicios basados en la web que permiten a los individuos:

1. Construir un perfil público o semipúblico dentro de un sistema con unos límites bien definidos.
2. Elaborar una lista de otros usuarios con los cuales uno está relacionado.
3. Navegar por la propia lista de usuarios o la de los demás.

Lo que hace a las páginas de redes sociales verdaderamente únicas no es que permitan a los individuos contactar con desconocidos, sino que los usuarios puedan conocer y dejar ver a los demás sus redes de amigos. Esto puede propiciar que se conozcan a individuos que, de otra forma, nunca hubieran entrado en contacto, lo que se denomina “vínculo latente”. Por otro lado, en muchas páginas de redes sociales, los usuarios no necesariamente buscan conocer gente nueva, sino que las utilizan principalmente para comunicarse con gente que ya forma parte de su red social.

Aunque las páginas de redes sociales hayan implementado una gran variedad de características técnicas, los perfiles que muestran la lista de amigos que también son usuarios del sistema son la base de su funcionamiento. Los perfiles son páginas únicas en las que cada uno “escribe lo que quiere ser”. Tras la inscripción a una red social, el usuario debe rellenar unos formularios que contienen una serie de preguntas. El perfil se genera utilizando las respuestas a estas preguntas, que suelen incluir elementos como la edad, ubicación, intereses, y una sección “sobre mí”. Asimismo se anima a los usuarios a que suban una foto de perfil. Algunas páginas permiten que los usuarios completen su perfil añadiendo contenido multimedia o modificando las características gráficas del perfil. Otras, como Facebook, permiten añadir módulos (aplicaciones).

La visibilidad de un perfil varía según la página y el criterio del usuario. Por defecto algunos aparecen incluso en buscadores como Google, aunque en general se puede configurar a quien se le permite el acceso al perfil. Las variaciones estructurales entorno a la visibilidad y al acceso de los perfiles es una de las diferencias fundamentales entre las distintas páginas de redes sociales.

Tras darse de alta en una web de redes sociales, se insta al usuario a identificar en el sistema a aquellos usuarios con los que esté relacionado. El nombre que se le da a esta relación varía según la página (“amigos”, “contactos”, o “fans”). En la mayoría de los casos se requiere confirmación bilateral para que se registre la relación entre dos personas en el sistema. Aunque existen lazos unidireccionales, los “fans”, generalmente aplicados a grupos.

El dominio público de las conexiones entre conocidos es un componente importante de las redes sociales. Las listas de amigos contienen enlaces a los perfiles de cada uno de ellos, por lo que se puede circular por el grafo de la red social simplemente haciendo clic en las listas de amigos. Normalmente la lista de amigos es visible para todo aquél que tenga permiso para ver el perfil, aunque hay excepciones.

La mayoría de estas redes también proporcionan un servicio para dejar mensajes en los perfiles de los amigos. Esto engloba los “comentarios” así como los mensajes privados, como si de un webmail se tratara. Más allá de los perfiles, amigos, comentarios y servicio de mensajes, las distintas páginas de redes sociales varían enormemente en cuanto a sus características y su orientación al usuario.

Algunas soportan el intercambio de fotos y video, otros se asemejan más a un blog. Otras se han creado específicamente para dispositivos móviles (Dodgeball), aunque la mayoría de las redes sociales ya tiene una versión para móvil. Algunas páginas están orientadas a personas de una determinada región geográfica o grupo lingüístico, o a algún grupo en concreto (según religión, sensibilidad política, orientación sexual u otras categorías). Existen incluso redes sociales para perros (Dogster) y gatos (Catster), aunque sean los dueños los que gestionen sus cuentas.

En definitiva, las páginas de redes sociales son unas páginas en las que se puede visitar los perfiles de amigos, o encontrar viejos amigos a través de la opción de búsqueda o navegando en las redes sociales de contactos que tengamos; unirse a redes y grupos de interés, publicar fotos y video, y en el caso de Facebook, usar diversas aplicaciones disponibles, incluso juegos.

b. Historia

Para entender cómo surgieron las redes sociales en la red, tendremos que remontarnos a principios de los años 90, cuando Internet era un medio puramente unilateral. La información se ofrecía a través de un formato estático, HTML. Se le podía dar formato al texto y añadir imágenes, navegar de una página a otra, pero no existía prácticamente interactividad entre los usuarios.

Entonces, algunas páginas web ofrecían a los usuarios la posibilidad de participar activamente mediante una página de contacto donde escribir comentarios, que se publicarían en la página en cuanto se actualizara. Cuando se empezó a utilizar Internet, la actualización de contenidos era una tarea tediosa y por tanto no se realizaba con mucha frecuencia. Los mensajes estaban lejos de publicarse en tiempo real, y había que depender siempre del administrador de la web. Si bien ya había cierta interacción entre los usuarios, ésta era todavía bastante pobre.

• Primeros foros, la semilla de los blogs

El desarrollo de nuevos lenguajes dinámicos como ASP y PHP hizo posible la creación de páginas web más interactivas en las que los usuarios, tras suscribirse, podían dejar sus comentarios relativos a temas elegidos por ellos mismos o los administradores. A estas webs se las denominó *Foros*, y su uso todavía está bastante extendido.

Hacia el año 2000 nació el lenguaje RSS, que sirvió de base para lo que se conoce comúnmente como blogs. La diferencia entre un blog y un foro es que generalmente en un blog escribe un único usuario (o un único grupo reducido de usuarios). Los suscriptores a estos blogs pueden añadir sus propios comentarios, pero no podrían añadir un nuevo tema como sucede en los foros. Otra diferencia importante entre los foros y los blogs es que, mientras que en el foro se debe acceder a la página para interactuar, se puede leer el contenido de los blogs a través de un lector RSS. De este modo, los temas que antes se trataban en un único foro se distribuyen a través de una red mucho más amplia, la *blogosfera*. Más adelante, en el año 2004, se enriqueció el formato de los blogs gracias a los *podcasts*, que permiten la difusión de medios más contundentes: archivos de sonido y de vídeo.

Esta nueva forma de relacionarse a través del contenido de una página web y las de otros suscriptores supuso la primera piedra para la Web 2.0, en la que el contenido de las páginas evoluciona constantemente mediante la implicación de comunidades on-line que comparten un interés común.

- **¿Cómo se llegó a las redes sociales?**

Ya existían perfiles en las webs de citas y otras comunidades y listas de amigos, pero no se podía ver los amigos de otros. Se podría considerar que la primera red social de Internet propiamente dicha surgió en 1997: SixDegrees.com. Esta web permitía crear perfiles, tener una lista de amigos y poder navegar por sus propias listas. Además tenía la opción de mandar mensajes a los amigos. Fue la primera página en combinar todos estos servicios. No obstante, a pesar de los millones de usuarios que consiguió atraer, dejó de ser rentable y cerró en el año 2000. Su creador siempre ha pensado que estaba adelantado a su tiempo.

En los años 1997 – 2001 siguieron surgiendo comunidades online que albergaban perfiles e incluían listas de amigos. En 2001 se lanzó Ryze.com, más bien orientada a negocios. Con ella nace la primera red social especializada, que en la actualidad agrupa a más de medio millón de profesionales. Basándose en el mismo concepto, LinkedIn es fundada a finales de 2002.

A partir de ese momento comenzó el verdadero auge de las redes sociales en Internet. Por no extendernos demasiado, veremos la cronología de las redes sociales más relevantes. En 2002 nace Friendster, la primera con un sistema inteligente capaz de relacionar a los usuarios de la red según sus gustos. Poco más tarde surge Fotolog, la primera red social que nace con el fin de intercambiar fotografías, seguida de Lastfm, en principio con el objetivo de ser una emisora en línea, pero con el tiempo se convierte en una red social movida por el interés en la música, del mismo modo que MySpace.

Cada vez son más numerosas y diversificadas las páginas de redes sociales. En 2004 surge Facebook, creada para el ámbito académico y universitario, actualmente líder omnipresente e indiscutible de las redes sociales con más de 500 millones de usuarios activos hasta la fecha¹. Otro hito en la historia de este tipo de páginas es la creación de Twitter en 2006, que revoluciona de nuevo el mundo de las redes sociales a través del concepto de *microblogging*, como veremos en el apartado 2.e.

¹ <http://www.facebook.com/press/info.php?statistics>

c. Tipos y clasificación de las redes sociales

Existe una gran diversidad de redes sociales en Internet. Podemos atenernos a cuatro criterios para clasificarlas. El primero y más general, es el grado de especialización. Algunas redes no tienen una finalidad concreta y de este modo aglomeran a una gran masa de gente, ideal para darle fuerza a una red social. Otras tienden a unir personas con aficiones comunes, como la música o los videojuegos, o ayudan a los usuarios a generar relaciones profesionales.

También podríamos clasificarlas según su contenido. Observamos que hay redes sociales que se centran en las relaciones entre las personas, muy distintas de las que presentan contenidos delegando los usuarios a un segundo plano, y por último las que relacionan entidades inanimadas, como marcas o incluso difuntos. La tercera clasificación que estudiaremos se basa en la importancia de la localización geográfica, ya que algunas webs varían según la cercanía geográfica entre usuarios o entre los usuarios y otros elementos. Y por último, cabe destacar que no algunas redes utilizan plataformas diferentes del web. Es el caso de los llamados *metaversos*, como Second Life, en los que los usuarios se relacionan del mismo modo que en las redes sociales del web, pero utilizando una base técnica diferente.

A continuación estudiaremos en detalle la comentada clasificación:

Horizontales / Verticales

- **Redes sociales Horizontales**

No tienen una temática definida y están dirigidas a todos los usuarios. Cualquiera puede registrarse y participar libremente sin un fin definido. Cada usuario elige el objetivo de su participación, aunque suelen centrarse en enviar mensajes, invitar, escribir comentarios y estar en contacto con los miembros de su red. Estas redes en definitiva tratan de reunir a una gran masa de gente que interactúe. Los ejemplos más típicos son Facebook o Twitter.

- **Redes sociales Verticales:**

Éstas giran en torno a un eje temático. Su objetivo es el de unir a un grupo de personas interesadas en un tema definido. En función de su especialización, podemos clasificar a su vez las redes sociales verticales en:

- **Redes sociales Verticales Profesionales**

Han sido diseñadas para generar relaciones profesionales y permitir un intercambio de información, y promocionar los distintos usuarios y empresas. Los ejemplos más representativos son Xing y LinkedIn.

- **Redes sociales Verticales de Ocio**

Unen a gente con aficiones comunes, como el deporte, videojuegos, música, etc. Los ejemplos más representativos son Dogster, Last.FM y Moterus.

- **Redes sociales Verticales Mixtas**

Ofrecen a usuarios y empresas un entorno específico para desarrollar actividades tanto profesionales como personales. Suelen incluir una agenda online o un buscador de servicios cercanos. Ejemplos de este tipo son PideCita y 11870.

Por el contenido:

- **Redes sociales Humanas**

Son aquellas que se centran en las relaciones entre personas uniendo individuos según su perfil social y en función de sus gustos, aficiones, lugares de trabajo, viajes y actividades. Ejemplos de este tipo de redes los encontramos en Youare y Tuenti.

- **Redes sociales de Contenidos**

En este caso se relacionan los perfiles a través de contenido publicado por los usuarios. Normalmente se trata de fotos, música o videos. Ejemplos más significativos son Flickr, Bebo, Friendster y FileRide.

- **Redes sociales de Inertes**

Suponen un enfoque novedoso en lo que a las redes sociales se refiere. Pueden unir marcas comerciales, lugares u objetos inanimados (como vehículos). Entre estas redes sociales destacan las de difuntos, siendo éstos los sujetos principales de la red. El ejemplo más llamativo es Respectance.

Por la importancia de la localización geográfica

- **Redes sociales Sedentarias**

Este tipo de red social muta en función de las relaciones entre personas, los contenidos compartidos o los eventos creados. Ejemplos de este tipo de redes son: Blogger, Bitacoras.com.

- **Redes sociales Nómadas**

A las características propias de las redes sociales sedentarias se le suma un nuevo factor de mutación o desarrollo basado en la localización geográfica del sujeto. Este tipo de redes se componen y recomponen a tenor de los sujetos que se hallen geográficamente cerca del lugar en el que se encuentra el usuario, los lugares que haya visitado o aquellos a los que tenga previsto acudir. Los ejemplos más destacados son: Latitud y Skout.

Algunos expertos consideran que las primeras redes sociales en consolidarse fueron los MMORPG (videojuegos de rol multijugador masivos en línea). Por lo tanto, también se podría añadir la plataforma como factor diferenciador de redes sociales:

Por su plataforma

- **Red Social MMORPG y Metaversos**

Normalmente contruidos sobre una base técnica Cliente-Servidor (WOW, Second Life, Lineage), pero no tiene por qué (Gladius, Travian, Habbo).

- **Red Social Web**

Su plataforma de desarrollo está basada en una estructura típica de web. Algunos ejemplos representativos son: MySpace y Hi5.

d. El impacto de las redes sociales en la sociedad

i. Todo un éxito entre los más jóvenes

Atrás quedan ya los tiempos en los que los jóvenes necesitaban salir de casa para relacionarse. Las redes sociales suponen una revolución de la comunicación entre niños y adolescentes, ya que ofrecen cientos de maneras de comunicarse sin la necesidad física de verse frente a frente. Gozan de una tremenda popularidad entre los menores, ya que, según un estudio realizado por la Universidad Camilo José Cela, el 70% de los adolescentes usa Tuenti². Al fin y al cabo, la red social no es más que una prolongación de su mundo, del grupo donde se siente comprendido y con el que se identifica.

Los hábitos de los adolescentes han cambiado notablemente respecto a los últimos años. Ya no pasan las tardes viendo la televisión o enganchados al teléfono. Hoy en día lo normal es que se pasen la tarde frente al ordenador, en la intimidad de su cuarto, lo cual puede dar la impresión errónea a los padres de que sus hijos se encierran en su mundo y no se relacionan. Nada más lejos de la realidad. Estas redes, lejos de aislarles, socializan todavía más a los jóvenes: controlan la comunicación con todas sus amistades a través de Internet y mediante determinados servicios conocidos como redes sociales, es decir que de hecho se pasan la tarde relacionándose³.

La falta de comprensión entre padres e hijos suele ser consecuencia de la llamada brecha digital, que se define como “la separación que existe entre las personas (comunidades, estados, países...) que utilizan las Tecnologías de Información y Comunicación (TIC) como una parte rutinaria de su vida diaria y aquellas que no tienen acceso a las mismas y que aunque las tengan no saben cómo utilizarlas.”⁴ Sólo el 37% de los progenitores tienen su propio perfil, y el 40% de los padres no saben que sus hijos tienen el suyo⁵. Estos datos se extraen del estudio ‘La juventud y las redes sociales en Internet’ elaborado por la Fundación Pfizer, para el que se ha entrevistado a 1.000 adolescentes y sus respectivos padres. En efecto, muchos padres ni siquiera conocen el significado de algunas de las palabras más utilizadas por sus hijos, como “tuenti” o “facebook”, pero aun sin saber a ciencia cierta qué es ese “nuevo invento” de las redes sociales, temen los riesgos para sus hijos.

Es justamente ese temor el que en ocasiones lleva a los padres a entrometerse directa o indirectamente en las redes sociales de sus hijos, como promueve Arturo Canalda, Defensor del Menor de la Comunidad de Madrid, que tiene un perfil en 'Tuenti' para controlar lo que hacen sus hijos en la red social⁶. Asegura que este control es “algo necesario a pesar de que puede resultar controvertido porque alguien puede entender que es vulnerar la intimidad de los hijos”. Esta polémica refleja el hecho de que la frontera entre la intimidad de los hijos y el control paterno se ha vuelto difusa.

² <http://www.ethek.com/el-70-de-los-adolescentes-usa-tuenti/>

³ <http://revista.consumer.es/web/es/20080601/Internet/72607.php>

⁴ Arturo Serrano, Evelio Martínez; “La Brecha Digital: Mitos y Realidades”

⁵ <http://www.facebooknoticias.com/2009/10/02/los-jovenes-y-las-redes-sociales-en-espana/>

⁶ <http://www.elmundo.es/elmundo/2010/03/12/madrid/1268412168.html>

Muchos jóvenes cuelgan toda su vida en Internet, y los padres pueden entrar en su red sin que nadie se dé cuenta y conocer detalles de sus hijos que de otro modo hubiera sido mucho más difícil descubrir. En pocas palabras, los padres disponen de tanta información sobre los jóvenes como sus propios amigos. Está claro que se puede justificar cierto control si es por brindar una mejor ayuda a los menores, pero por otro lado resulta poco ético invadir su intimidad. Además de sobreprotegerlos, podría resultar una actitud contraproducente y asfixiante para los jóvenes.

De todos modos, los aspectos positivos de las redes sociales para los jóvenes son muchos, y compensan todos los posibles peligros. Suponen una segunda oportunidad para aquellos que en el mundo exterior no logran comunicarse con su entorno, permiten compartir contenidos de manera constante y, de ese modo, también conocimientos. Como veremos en el apartado 4, una posible aplicación para las redes sociales es la docencia: permiten aprender y trabajar en equipo. Otra gran ventaja es que permiten familiarizarse de un modo lúdico con las nuevas tecnologías, que de otro modo quizás no usarían. Y aunque es cierto que existen ciertos peligros, las propias redes incluyen estrictos controles de privacidad y de contenidos para evitar esta situación (límites de edad, botones de aviso de contenidos molestos, las cláusulas de responsabilidad...).

ii. Una nueva forma de relacionarse

La irrupción de Internet en nuestras vidas ha dado paso a una forma virtual de relacionarse, de compartir nuestras experiencias de una forma mucho más global y generalizada, y sobretodo más cómoda.

Ya no hace falta pedirle copias de las fotos a nadie: es tan sencillo como entrar en un perfil de Facebook sin movernos de la silla. Se puede etiquetar a los contactos que aparecen en una foto e incluso hacer comentarios, como si se tratara de una reunión en la vida real, y sin importar la distancia física de los participantes. Este hecho concreto sustituiría un acto social real hasta ahora habitual: una quedada de amigos para ver y comentar las fotos de una noche o un viaje, por ejemplo.

Por tanto, vemos que las redes sociales han distribuido los flujos de comunicación hacia nuevas vías. Según una encuesta en diferentes países europeos incluida España, el teléfono fijo ha pasado a un segundo lugar frente a la comunicación en las redes sociales. Del mismo modo, se aprecia un descenso en el uso de servicios de mensajería instantánea tradicionales como MSN Messenger o ICQ, ya que los usuarios de redes sociales disponen de una aplicación de mensajería integrada.

La mencionada integración es una de las claves del éxito de las redes sociales. El usuario es vago por naturaleza, y prefiere tener todas las opciones de comunicación incluidas en un mismo lugar. Si puede, utilizará la opción de chat en lugar del Messenger, y los mensajes en lugar del e-mail. Su red de amigos sustituye su agenda de contactos. Y lo más interesante, es que la comunicación siempre fluye de inmediato, y se puede elegir si es privado (mensaje a un usuario) o público (mensaje en el muro de Facebook, por ejemplo). En tal caso, una red social se puede utilizar como escaparate para que cada uno publique lo que quiera de sí mismo.

Un fenómeno especialmente curioso que ha aparecido con las redes sociales, es el reencuentro de antiguos compañeros de clase largamente olvidados, el cual se ha analizado en profundidad en un artículo del diario El País⁷. El ímpetu nostálgico por reencontrar antiguos compañeros siempre ha existido, pero ahora es más fácil. Como ya no hace falta rebuscar el teléfono de la casa de los padres de nadie, ahora sí se retoma el contacto con viejos conocidos. Lo hacen por curiosidad, por nostalgia o por necesidad de sentirse parte de un grupo. De cualquier manera, las redes sociales permiten reactivar relaciones latentes.

Por último, las redes de personas no son un simple directorio de los amigos de la vida real, también pueden ayudar a encontrar nuevas amistades, trabajo o nuevos socios. En las redes sociales cada uno muestra un escaparate con lo que desea que vean los demás. Pero habrá que tener en cuenta que, entre el grupo de espectadores de nuestra vida cotidiana puede encontrarse gente con la que no se desea compartir estados de ánimo o fotos comprometidas. Esto obliga a tener cuidado a la hora de agregar nuevos amigos a la red, así como a gestionar eficientemente las amistades y opciones de privacidad que brindan las distintas plataformas.

iii. Un nuevo poder mediático

Los medios de comunicación tradicionales, también conocidos como *mass media*, se ven amenazados por una nueva manera de difundir la información – los *social media*. En la Web 2.0, la producción deja de estar en manos de un elemento central, que suele ejercer un poder de filtro, para pasar a la de los usuarios, con libertad - a priori absoluta - de publicar lo que les parece.

En particular, las redes sociales y la blogosfera han causado estragos en los portales puntocom y grandes proveedores de contenido que se limitaban a replicar, en versión electrónica, el ecosistema mediático descentralizado del siglo XX⁸. Frente a los *mass media*, que presentan una estructura centralizada, las redes forman una estructura distribuida que imposibilita la aplicación de filtros externos. Esto acarrea consecuencias evidentes para las formas tradicionales de poder, que se apoyaban en los medios de comunicación convencionales.

Este cambio en el paradigma de los medios de comunicación se hace patente en una entrevista realizada por el diario El País a Daniel Ellsberg⁹ – responsable de filtrar a la prensa los papeles del Pentágono en 1971, relativos a la guerra de Vietnam. Si le preguntamos al Sr. Ellsberg qué habría hecho hoy, en la era de las redes e Internet, responde sin dudar: “compraría un escáner y los subiría en Internet”.

Hoy en día ya no es necesario pasar por los filtros de los medios de comunicación para hacer pública una información. Basta con ponerla en manos de la opinión pública y dejar que la presión surja de allí. Y con las herramientas de las que disponemos ahora, nunca había sido tan fácil. Un nuevo y complejo ecosistema informativo está emergiendo de Internet y de las redes sociales, lo que otorga

⁷ ¿Me ‘ajuntas’?, versión 2.0. El País. 01/08/2010.

⁸ El Poder de las Redes. David de Ugarte.

⁹ El nuevo ecosistema de la información. El País Opinión. 9/8/2010.

posibilidades virtualmente ilimitadas de difundir información. Los *mass media* dejan de ser elementos centrales, y dan paso a nuevas organizaciones capaces de retar y poner en riesgo la seguridad del Estado.

A continuación analizaremos algunas características que ayudan a mostrar las diferencias entre los medios sociales y los medios de masas¹⁰:

- **Audiencia:** Si nos limitamos a las ediciones digitales, ambos medios permiten a cualquier persona acceder a los contenidos desde un ordenador, de modo que en los dos casos pueden llegar a una audiencia global.
- **Acceso:** Los medios de masas son generalmente de pago y son propiedad de un particular o del gobierno, mientras que los medios sociales están en general disponibles para cualquier persona con poco o ningún costo.
- **Facilidad de uso por los creadores:** En los medios industriales la producción del contenido requiere normalmente de recursos y conocimientos especializados. La mayoría de los medios sociales no, o en algunos casos se reinventa habilidades, de modo que cualquier persona puede ser un productor en estos medios.
- **Instantaneidad:** El tiempo que transcurre entre la producción del contenido y su entrega a las audiencias puede ser largo (días, semanas o incluso meses) en comparación con los medios sociales (que puede ser capaz brindar contenido prácticamente de forma instantánea o sólo con muy pequeños retrasos en su publicación). Los medios industriales están evolucionando con la adopción de recursos y tecnologías de modo que esta característica puede no ser la más distintiva en poco tiempo.
- **Edición del contenido:** En los medios industriales, una vez creado el contenido éste no puede ser alterado (una vez que el artículo de una revista se ha impreso y distribuido los cambios no se pueden hacer en ese mismo artículo), mientras que los medios sociales no sólo se enriquecen con los comentarios de las audiencias, sino que el contenido puede ser alterado instantáneamente por los productores, mejorando en contenido para las audiencias.

¹⁰ E-marketing y social media 2010. Universidad Autónoma de Chihuahua.

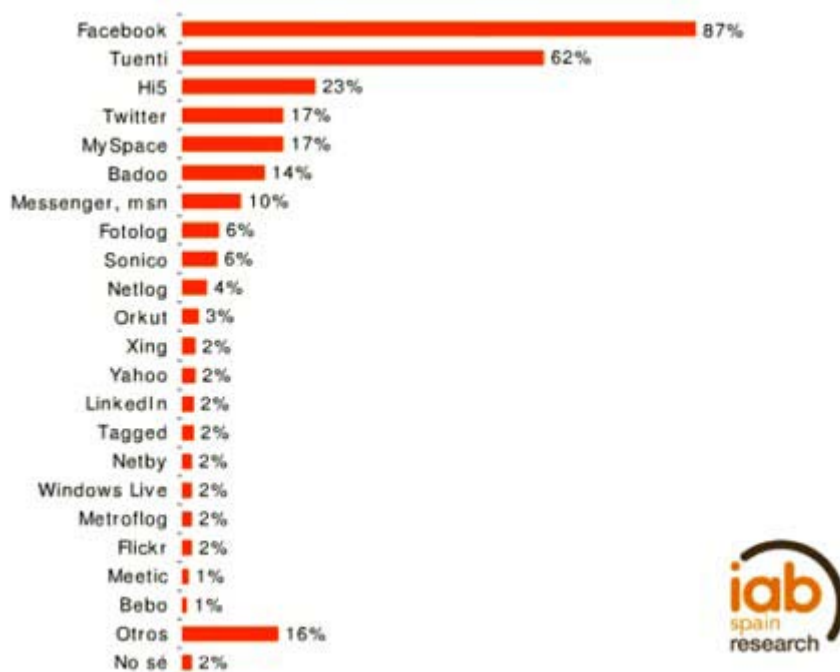
	Medios de masa	Medios sociales
Audiencia	Global	Global
Acceso	Generalmente de pago	Generalmente gratuitos
Facilidad de uso	Requiere recursos y conocimientos especializados	Cualquier persona puede ser productora.
Instantaneidad	Transcurre un tiempo largo entre la producción de contenido y la entrega a las audiencias (cada vez menor).	Brinda contenido de forma instantánea.
Edición del contenido	Imposible alterar el contenido.	El contenido puede ser alterado instantáneamente por los productores, y se enriquece con comentarios de las audiencias.

Tabla: Diferencias fundamentales entre medios de masa y medios sociales

Los medios sociales ejercen una presión positiva sobre los gobiernos, al exigirles transparencia y apertura. No obstante, la falta de regulación que los caracteriza permite un uso poco ético de los medios hasta ahora bloqueado por los medios convencionales en los estados democráticos. Como cualquiera puede usar los medios sociales, se abre la puerta a grupos terroristas o del crimen organizado, especuladores financieros o grupos de interés, que emplearan la red para alcanzar sus objetivos. El mayor atractivo de las redes –anonimato, viralidad, interconexión– es también su mayor debilidad. Se pueden utilizar en cualquier sentido y para cualquier propósito, ya que escapan a cualquier tipo de control.

e. Las redes sociales más utilizadas

Dada la gran variedad de páginas dedicadas a las redes sociales en Internet, nos centraremos principalmente en tres de las redes más notorias en nuestro país: Facebook (10 millones de usuarios activos), Tuenti (8 millones) y Twitter (5 millones).



Como figura en un reciente informe de IAB Spain¹¹ – asociación que representa al sector de la publicidad digital en España – Facebook y Tuenti son de largo las redes más utilizadas en España. Vendrían seguidas por Hi5, Twitter y MySpace. Hemos optado por analizar Twitter ya que se trata de una red social peculiar, que hace uso del micro-blogging, y aunque se encuentre la cuarta en la lista está experimentando un gran crecimiento en este momento.

i. Facebook



Facebook es una página web gratuita de redes sociales operativa desde el año 2004, propiedad de la compañía Facebook Inc. La compañía tiene sus oficinas centrales en Palo Alto, California. Tiene más de 500 millones de usuarios activos en septiembre de 2010.

Los usuarios pueden añadir amigos y enviarles mensajes, así como actualizar su perfil personal para mostrarlo a sus amigos. Además, los usuarios pueden unirse a redes organizadas según su lugar de trabajo, escuela, universidad... El nombre de la

¹¹ <http://www.iabspain.net/blog/?p=51>

web proviene del nombre que se le da coloquialmente al libro que se entrega a los estudiantes al inicio del curso académico en las universidades de los EEUU, a fin de ayudar a los estudiantes a conocerse mejor entre ellos. Facebook admite como miembro a cualquier persona mayor de 13 años (salvo en el caso concreto de España, donde debe ser mayor de 14 años).

Facebook fue fundada por Mark Zuckerberg y sus compañeros de carrera. En principio, la entrada de miembros se limitaba a estudiantes de la Universidad de Harvard, pero se fue expandiendo gradualmente, añadiendo estudiantes de otras universidades. Después se permitió el uso a estudiantes de instituto, hasta aceptar a cualquier persona mayor de 13 años con una cuenta de correo electrónico.

A mediados de 2007 lanzó las versiones en francés, alemán y español para impulsar su expansión fuera de Estados Unidos, ya que sus usuarios se concentraban en Estados Unidos, Canadá y Gran Bretaña. En enero de 2010, Facebook contaba con 380 millones de miembros, y traducciones a 70 idiomas.

La fortaleza de la red social Facebook radica en los ya 500 millones de usuarios que ha conseguido, basada en conexiones de gente real. Los usuarios pueden participar en una o más redes sociales, en relación con su situación académica, su lugar de trabajo o región geográfica. Casi cualquier persona con conocimientos informáticos básicos puede tener acceso a todo este mundo de comunidades virtuales.

Facebook compite por abrirse espacio entre empresas de éxito como Google y MySpace, por lo que se enfrenta a grandes desafíos para lograr crecer y desarrollarse. Una de las estrategias de Zuckerberg ha sido abrir la plataforma Facebook a otros desarrolladores.

La página no está carente de controversia. Su uso se ha bloqueado en varios países, como Paquistán, Siria, China, Vietnam e Irán. También se ha prohibido el acceso en muchos lugares de trabajo para evitar que los empleados malgasten su tiempo. Existe una gran polémica en torno a la privacidad, y se ha llevado a la compañía a juicio por asuntos de propiedad intelectual. Por último, se ha acusado a Facebook de vender datos de fans y amigos.

La mayor parte de los ingresos de Facebook proceden de los Créditos – moneda virtual que los usuarios utilizan para comprar bienes virtuales en juegos y aplicaciones de Facebook – y los anuncios que aparecen a un lado de la página. Sin embargo, Facebook tiene una tasa de cliqueo significativamente más baja que otras webs importantes. Microsoft es el socio exclusivo de Facebook para la publicidad en banners, es decir, Facebook sólo publica anuncios de la lista de anunciantes de Microsoft.

Según comScore, una empresa de investigación de marketing, Facebook recopila tanta información de sus visitantes como Google o Microsoft, aunque considerablemente menos que Yahoo!. En 2010, el equipo encargado de la seguridad aumentó sus esfuerzos para luchar contra las amenazas a los usuarios y el terrorismo.

En enero de 2009, un estudio de Compete.com situó a Facebook como la red social más utilizada, en cuanto a usuarios activos a nivel mundial, seguida de MySpace.

- **Servicios que ofrece**

Lista de Amigos: En ella el usuario puede agregar a cualquier persona que conozca y esté registrada, siempre que acepte su invitación. En Facebook se pueden localizar amigos con quienes se perdió el contacto o agregar otros nuevos con quienes intercambiar fotos o mensajes. Para ello, el servidor de Facebook posee herramientas de búsqueda y de sugerencia de amigos.

Grupos y Páginas: Es una de las utilidades de mayor desarrollo reciente. Se trata de reunir personas con intereses comunes. En los grupos se pueden añadir fotos, vídeos, mensajes, etc. Las páginas, se crean con fines específicos y a diferencia de los grupos no contienen foros de discusión, ya que están encaminadas hacia marcas o personajes específicos y no hacia ningún tipo de convocatoria.

Muro: el muro (*wall* en inglés) es un espacio en cada perfil de usuario que permite que los amigos escriban mensajes para que el usuario los vea. Sólo es visible para usuarios registrados, muro te permite ingresar imágenes y poner cualquier tipo de logotipos en tu publicación. Una mejora llamada supermuro permite incrustar animaciones flash.

Fotos: Según Facebook, hay 5 mil millones de fotos de usuario y 160 terabytes de almacenaje.

Regalos: los regalos o *gifts* son pequeños íconos con un mensaje. Los regalos dados a un usuario aparecen en la pared con el mensaje del donante, a menos que el donante decida dar el regalo en privado, en cuyo caso el nombre y el mensaje del donante no se exhiben a otros usuarios.

Juegos: Entre los más célebres se encuentran los juegos de Playfish y los juegos de Zynga Games como Farmville.

La proliferación de juegos, tests y actividades secundarias a la red social en sí que dificultan a veces las funciones principales de comunicación. Hay muchos grupos de personas cansados de tener que cultivar una granja, dar de comer a los peces, crear un imperio criminal etc.

Facebook ha recibido todo tipo de críticas desde que alcanzó difusión global, debido al alcance que está teniendo entre menores, sus efectos psicológicos y sus alarmantes políticas de privacidad.

ii. Tuenti



Tuenti es una red social virtual dirigida a la población joven española. Permite al usuario crear su propio perfil, subir fotos y vídeos y contactar con amigos. Tiene otras muchas posibilidades como crear eventos y etiquetar amigos en fotos.

Inaugurado en enero de 2006, Tuenti es uno de los sitios web más visitados en España, según Alexa Internet. Fue creada en 2006 por Zaryn Dentzel, un estudiante estadounidense actualmente afincado en Madrid (España). Dentzel conoció España a través de un intercambio que lo llevó a Cabeza del Buey (Badajoz) y, a raíz de esta experiencia, fue como años más tarde nacería Tuenti.

Al igual que Facebook, al principio iba dirigido para universitarios y sólo algunos conocidos pudieron probarlo. Más tarde, en vista de su éxito, permitieron la entrada a más usuarios, pero sólo si tenían invitación. Actualmente se calcula que tiene 6 millones de usuarios en España, la inmensa mayoría de ellos universitarios y colegiales. Según Zaryn Denzel, el nombre “Tuenti” surgió de la necesidad de encontrar uno que incluyera “tú” y “ti”. Para ponerle nombre los miembros barajaron muchos nombres y al final escogieron Tuenti porque se parece a “tu entidad” y porque sonaba bien.

Tuenti es una red social de acceso restringido a la que sólo se entra mediante la invitación de un miembro anteriormente registrado. Este mecanismo, según la empresa, garantiza en principio que todo usuario recién llegado ya tenga un vínculo con otro miembro de la red a partir de cual pueda empezar a establecer relaciones con el resto de los usuarios.

- **Servicios que ofrece**

Mi perfil

Cada usuario dispone dentro de la red de una página denominada “Mi perfil” dividida en varios apartados cuya visibilidad dentro de la red por el resto de los usuarios puede ser regulada de manera que sólo sea visible por los amigos del usuario, por los amigos de sus amigos o por todos los usuarios. En esta página se encuentra normalmente en la columna izquierda una fotografía del usuario con información personal tal como el sexo, la edad, el estado actual (a elegir entre “soltero”, “con alguien”, “con rollo”), la fecha de cumpleaños, la ciudad de residencia, lo que el usuario busca dentro de la red (“amistad”, “chico/chica”, “chico/chica para rollo”) y la fecha de ingreso. Se incluye además en esta misma columna información sobre los intereses del usuario como sus aficiones, sus películas y libros preferidos, sus grupos de música favoritos, y los sitios que suele frecuentar.

La columna central de “Mi Perfil” está dividida en dos bloques: el blog y “Mi tablón”. La sección de blog proporciona al usuario un espacio donde escribir textos e incluir vídeos a modo de blog, ordenando las entradas por orden cronológico inverso. “Mi tablón” es un espacio donde los demás usuarios de la red pueden dejar mensajes personales y también donde se puede visualizar el historial de estados. El nuevo historial de estados contiene las actualizaciones de estado que estuvo haciendo la persona recientemente.

Finalmente, la columna derecha muestra tres listas reducidas: uno de ellos es una lista de las últimas ocho fotos en la que está etiquetado el usuario, y otras dos listas de los amigos del usuario ordenada según la fecha de actualización de sus perfiles y otra lista más reducida de los amigos en común con tu lista de amigos.

Buscador

Tuenti dispone de un buscador para localizar a todos los miembros de la red por su nombre real. Para reducir los resultados de la búsqueda se dispone de varios filtros como el sexo, la edad, el centro de estudios o trabajo y la zona de marcha.

Chat

La red social Tuenti estrenó en Septiembre de 2009 una nueva función de chat mediante la que los usuarios podrán establecer conversaciones y en tiempo real con sus contactos al estilo de los servicios de chat de Terra. De este modo, los usuarios podrán mantener un contacto más fluido entre ellos y disponer de una nueva herramienta con que canalizar las más de 7 millones de conversaciones nuevas que se establecen cada día en Tuenti, según su director de comunicación, Ícaro Moyano.

La herramienta aparece en una ventana en la esquina inferior izquierda y el internauta puede navegar por los perfiles de sus contactos, subir fotos o publicar vídeos mientras charla con sus amigos. También ofrece la posibilidad de bloquear aquellos contactos con quienes no se quiera establecer conversación.

Esta novedad llega meses después del último rediseño de la página y de la reciente incorporación a la compañía de Koro Castellano —ex directora general de Internet en Unidad Editorial—, en un desesperado intento por seguir adelante en su batalla contra Facebook, una red social tecnológicamente más avanzada que cuenta con el respaldo de más de 500 millones de usuarios repartidos por todo el mundo.

A Tuenti se le suele acusar de simpleza y de escasez de opciones en ciertos campos, sin embargo cumple holgadamente su cometido a la hora de colgar y compartir fotos. Por otro lado, si de algo presume Tuenti es de su política de privacidad ya que no permiten la inclusión de contenidos personales en buscadores como Google.

iii. Twitter



A pesar de llegar algo más tarde que Facebook, Twitter, se ha convertido, con un temprano crecimiento del 750 por ciento, en una de las herramientas esenciales de los denominados *social media*. De hecho, supone un nexo de unión entre los *social media* y las redes sociales propiamente dichas.

Twitter es como un blog de “status” como el que se emplea en Facebook. El usuario teclea pensamientos o acciones de un determinado momento. La diferencia radica en la limitación de 140 caracteres de Twitter, que obliga a reducir el texto a lo esencial. El envío de estos mensajes se puede realizar tanto por el sitio web de Twitter, como vía SMS desde un teléfono móvil, desde programas de mensajería instantánea, o incluso desde cualquier aplicación de terceros. Esto dota a la página de un gran dinamismo.

Estas actualizaciones se muestran en la página de perfil del usuario, y son también enviadas de forma inmediata a otros usuarios que han elegido la opción de recibirlas. A estos usuarios se les puede restringir el envío de estos mensajes sólo a miembros de su círculo de amigos o permitir su acceso a todos los usuarios, que es la opción por defecto.

Desde que Twitter ganó más popularidad, muchas celebridades desde personajes destacados a actores de Hollywood se unieron al *microblogging*. A los *twitteros* más conocidos se le llaman *Twitterati*, que son usuarios muy leídos o influyentes. Muchos de ellos captan la atención y aparecen en los *Temas del Momento*. Es diferente a los *twitteros* que se encargan de escribir su vida cotidiana cada minuto, aunque el usuario no tenga muchos seguidores.

Twitter también ha sido objeto de muchas críticas. Existen detractores del formato de 140 caracteres: para mucha gente, la idea de describir constantemente el día a día es absurdo. En cuanto a las posibles noticias que se publican, se detectan muchos bulos, además de una gran cantidad de spam. Por último, no hay que olvidar el gran problema inherente a las redes sociales, la preocupación por la privacidad, ya que se ha acusado a Twitter de compartir información personal con terceros.



3. Aspectos legales de la informática

a. Marco general

En este apartado estudiaremos los instrumentos legales existentes susceptibles de regular las redes sociales a nivel internacional, europeo y por último nacional. Nos centraremos principalmente en los documentos relacionados con la privacidad, la propiedad intelectual y los servicios ofrecidos por Internet.

i. Convenios internacionales

- **Privacidad**

Hay una gran variedad de leyes relacionadas con la privacidad a nivel mundial. En este apartado trataremos de recopilar los instrumentos internacionales más relevantes para el respeto de la privacidad de las personas de aplicación en todos los países.

El derecho a la vida privada de un modo general se contempla en distintos documentos oficiales de la Organización de las Naciones Unidas. En primer lugar, se menciona en la **Declaración Universal de los Derechos Humanos**¹² (ONU, 1948):

Artículo 12.

Nadie será objeto de injerencias arbitrarias en su vida privada, su familia, su domicilio o su correspondencia, ni de ataques a su honra o a su reputación. Toda persona tiene derecho a la protección de la ley contra tales injerencias o ataques.

El Pacto Internacional de Derechos Civiles y Políticos¹³ (ONU, 1966) incluye el mismo texto en su artículo 17. Esta ley viene ampliada por la Convención sobre los Derechos del Niño¹⁴ (ONU, 1989), con un artículo idéntico al anterior pero aplicado a los niños.

Artículo 16.

1. *Ningún niño será objeto de injerencias arbitrarias o ilegales en su vida privada, su familia, su domicilio o su correspondencia ni de ataques ilegales a su honra y a su reputación.*
2. *El niño tiene derecho a la protección de la ley contra esas injerencias o ataques.*

¹² <http://www.un.org/es/documents/udhr/>

¹³ http://ec.europa.eu/justice/policies/privacy/docs/16-12-1996_en.pdf

¹⁴ <http://www.margen.org/ninos/derech8b.html>

Además, existen unas directrices establecidas por la ONU que afectan a los ficheros informatizados de datos de carácter personal, denominada, en inglés, **United Nations Guidelines concerning Computerized Personal Data Files (14/12/90)**. Esta guía contiene orientaciones sobre los procedimientos para regular los ficheros de datos personales. Le corresponde a cada estado aplicar los procedimientos pertinentes para llevar a cabo dichas regulaciones.

Se establecen diez principios para otorgar unas garantías mínimas en las legislaciones nacionales, como se puede apreciar en el siguiente resumen.

United Nations Guidelines concerning Computerized Personal Data Files

1. Principio de legalidad y legitimidad

La información sobre las personas no debe recogerse de forma ilegal o ilegítima, ni puede emplearse para fines contrarios a los establecidos en la Carta de las Naciones Unidas.

2. Principio de veracidad

Se debe comprobar regularmente la veracidad y la relevancia de los datos, que deben ser lo más completa posible para evitar errores por omisión

3. Principio de especificación de la finalidad

La finalidad debe ser especificada, legítima para asegurar los siguientes puntos:

- i. Los datos deben ser relevantes y adecuados a la finalidad*
- ii. Se prohíbe el uso de los datos para fines incompatibles*
- iii. El periodo de almacenamiento de los datos no puede exceder de la consecución de la finalidad*

4. Principio de acceso de la persona interesada

Cualquier persona debidamente identificada tiene derecho a acceder a su información y a rectificarla. Los costes correrán a cuenta del responsable del fichero.

5. Principio de no-discriminación

Salvo las excepciones contempladas en el apartado 6, no se deberían incluir datos susceptibles de provocar discriminación (raza, religión, vida sexual, opiniones políticas...)

6. Capacidad de hacer excepciones

Se pueden hacer excepciones a los principios citados para preservar la seguridad nacional, el orden público, la salud pública...

7. Principio de seguridad

Se deberán tomar las medidas adecuadas para proteger los ficheros frente a pérdidas y accesos no autorizados.

8. Supervisión y sanciones

Cada estado designará las autoridades responsables de supervisar el cumplimiento de los principios establecidos, pudiendo aplicar las sanciones pertinentes.

9. Transacción de datos a través de fronteras

En caso de intervenir dos estados distintos en una transacción de datos, la información debe poder circular libremente en cualquiera de los territorios involucrados.

10. Campo de aplicación

Estos principios se aplican a todos los ficheros informatizados públicos y privados, así como a ficheros manuales.

Del mismo modo, la Organización para la Cooperación y el Desarrollo Económico ha establecido sus propias directrices, así como una serie de recomendaciones complementarias, en el documento **Directrices de la OCDE para la Seguridad de Sistemas y Redes de Información: hacia una cultura de seguridad**.

Directrices de la OCDE para la Seguridad de Sistemas y Redes de Información

1. Concienciación

Los participantes deberán ser conscientes de la necesidad de contar con sistemas y redes de información seguros, y tener conocimiento de los medios para ampliar la seguridad.

2. Responsabilidad

Todos los participantes son responsables de la seguridad de los sistemas y redes de información.

3. Respuesta

Los participantes deben actuar de manera adecuada y conjunta para prevenir, detectar y responder a incidentes que afecten la seguridad.

4. Ética

Los participantes deben respetar los intereses legítimos de terceros.

5. Democracia.

La seguridad de los sistemas y redes de información debe ser compatible con los valores esenciales de una sociedad democrática.

6. Evaluación del riesgo

Los participantes deben llevar a cabo evaluaciones de riesgo.

7. Diseño y realización de la seguridad.

Los participantes deben incorporar la seguridad como un elemento esencial de los sistemas y redes de información.

8. Gestión de la Seguridad.

Los participantes deben adoptar una visión integral de la administración de la seguridad.

9. Reevaluación

Los participantes deben revisar y reevaluar la seguridad de sus sistemas y redes de información, y realizar las modificaciones pertinentes sobre sus políticas, prácticas, medidas y procedimientos de seguridad.

Además, la OCDE ha presentado otros documentos como las **Guías que Regulan la Protección de la Privacidad y los Flujos Transfronterizos de Datos Personales**, muy similar al documento de la ONU sobre la protección de datos personales informatizados, o la **Declaración Ministerial sobre Protección de la Privacidad en las Redes Globales**, que vienen a apoyar estas directrices de forma exhaustiva y más adaptada a la situación actual.

Sin embargo, conviene señalar que, tanto las directrices de Naciones Unidas como las de la OCDE, al tratarse de meras directrices, carecen de valor vinculante y obligatorio. Éstas únicamente proponen un marco general de actuación de los diferentes estados miembros de esas organizaciones internacionales a la hora de abordar la regulación de la privacidad. Es por tanto de esperar que, tanto organizaciones internacionales que disponen de instrumentos con carácter obligatorio (por ejemplo, la Unión Europea), o los propios estados, adopten medidas que se adecúen a estas directrices, pero no están obligados a ello. Por tanto, estas directrices sirven no sólo de fuente de inspiración de las legislaciones nacionales sino también como orientación a la hora de interpretar las mismas.

Acuerdo de Puerto Seguro

No existe, dado el marcado carácter auto-regulador del comercio en Estados Unidos, una normativa sobre protección de datos de carácter personal aplicable en todo el territorio y en todos los sectores de actividad, sino a lo sumo normas dispersas aplicables a sectores muy concretos.

A fin de superar los problemas derivados de esta dispersión normativa, el Departamento de Comercio de los Estados Unidos presentó, como documento para la discusión entre las autoridades norteamericanas y de la Unión Europea un borrador de "principios de puerto seguro", a fin de garantizar a los operadores que se adhirieran a los mismos una "presunción de adecuación" al nivel de protección exigido por la Directiva, permitiéndose así la libre transferencia internacional de datos a dichos operadores.

La Comisión Europea, mediante su Decisión de 26 de julio de 2000, y con arreglo a la Directiva 95/46/CE del Parlamento Europeo y del Consejo, se pronunció sobre la adecuación conferida por los principios de puerto seguro para la protección de la vida privada y las correspondientes preguntas más frecuentes, publicadas por el Departamento de Comercio de Estados Unidos de América.¹⁵

• Propiedad Intelectual e Industrial

La **Organización Mundial de la Propiedad Intelectual (OMPI)** protege nuevos inventos a través de las patentes y mantiene un registro de casi tres millones de marcas registradas. También protege mediante tratados de ámbito de aplicación internacional las obras de artistas, compositores y autores en todo el mundo. La labor de la OMPI hace más fácil y más barato que individuos y empresas hagan respetar sus derechos de propiedad. También amplía las oportunidades de distribuir nuevas ideas y productos sin renunciar al control sobre los derechos de propiedad.

La OMPI tiene a su cargo la administración de 24 tratados internacionales que abordan diversos aspectos de la regulación de la propiedad intelectual. Existen convenios para la protección de la propiedad intelectual desde hace más de un siglo. El **Convenio de Berna para la Protección de las Obras Literarias y Artísticas** (1886) y el **Convenio de París para la Protección de la Propiedad Industrial** (1883) siguen sentando las bases del sistema de tratados de la OMPI. Los tratados firmados en años posteriores, que son el **Tratado de la OMPI sobre Derecho de Autor (WCT)** y el **Tratado de la OMPI sobre Interpretación o Ejecución y Fonogramas (WPPT)** han ampliado y profundizado el alcance de la regulación y han incorporado los cambios tecnológicos y nuevas esferas de interés.

El convenio de Berna se apoya en tres principios básicos, como podemos apreciar en el siguiente recuadro.

Convenio de Berna

1. *Las obras originadas en alguno de los estados contratantes podrán recibir en cada uno de los demás estados contratantes la misma protección que estos otorgan a las obras de sus propios ciudadanos.*
2. *Esa protección no debe estar condicionada al cumplimiento de formalidad alguna.*
3. *Esa protección es independiente de la existencia de una protección correspondiente en el país de origen de la obra. Sin embargo, si un estado contratante provee un plazo más largo que el mínimo prescrito por la convención, y la obra deja de estar protegida en el país de origen, la protección le puede ser negada una vez que cese la protección en el país de origen.*

¹⁵ Fuente: Agencia Española de Protección de Datos (<http://www.agpd.es>)

El convenio de París se centra en la propiedad Industrial. Aunque proteja especialmente a las marcas, también incluye inventos, diseños industriales, modelos de uso práctico, nombres comerciales, denominaciones geográficas y la represión de la competencia desleal.

ii. Legislación europea

• Privacidad

El primer documento europeo relativo a la privacidad se conoce como Convenio Europeo para la Protección de los Derechos Humanos y Libertades Fundamentales¹⁶ (1950).

Artículo 8. Derecho al respeto a la vida privada y familiar.

1. *Toda persona tiene derecho al respeto de su vida privada y familiar, de su domicilio y de su correspondencia.*
2. *No podrá haber injerencia de la autoridad pública en el ejercicio de este derecho, sino en tanto en cuanto esta injerencia esté prevista por la ley y constituya una medida que, en una sociedad democrática, sea necesaria para la seguridad nacional, la seguridad pública, el bienestar económico del país, la defensa del orden y la prevención del delito, la protección de la salud o de la moral, o la protección de los derechos y las libertades de los demás.*

La diferencia fundamental entre el Artículo 12 de la **Declaración de los Derechos Humanos** de la ONU y este artículo del Consejo de Europa radica en que este último justifica una injerencia en la privacidad de las personas si se considera necesaria para mantener el bienestar común y siempre y cuando se halle prevista por la legislación ya sea europea o nacional.

En 1981, coincidiendo con la ratificación de las reglas de la OCDE, se aprueba el **Convenio para la protección de individuos con respecto al proceso automático de datos personales**¹⁷ en el Consejo de Europa. Este extiende la protección del ciudadano así como sus libertades fundamentales, en particular el derecho al respeto de su vida privada, tomando en cuenta el aumento de los flujos, nacionales e internacionales, de datos de carácter personal a través del tratamiento automatizado. Este convenio ha inspirado en gran parte la directiva 95/46/CE de la Comisión Europea de 1995 al respecto, sobre la que se apoya la LOPD española de la que hablaremos en el siguiente apartado.

¹⁶ http://www.ruidos.org/Normas/Conv_europeo_dchos_hum.htm

¹⁷ <http://conventions.coe.int/Treaty/en/Treaties/Html/108.htm>

Por último, veremos dos artículos de la Carta de los Derechos Fundamentales de la Unión Europea (2000) que, aparte de lo establecido en otros convenios anteriores sobre los derechos de los ciudadanos a la privacidad, a la protección de sus datos y al acceso a sus datos, contempla que el control de estas reglas deberá llevarse a cabo por una autoridad independiente que se designará en cada estado. Es el caso de la Agencia Española de Protección de Datos en nuestro país.

Carta de los Derechos Fundamentales de la Unión Europea

Artículo 7

Respeto de la vida privada y familiar

Toda persona tiene derecho al respeto de su vida privada y familiar, de su domicilio y de sus comunicaciones.

Artículo 8

Protección de datos de carácter personal

- 1. Toda persona tiene derecho a la protección de los datos de carácter personal que la conciernan.*
- 2. Estos datos se tratarán de modo leal, para fines concretos y sobre la base del consentimiento de la persona afectada o en virtud de otro fundamento legítimo previsto por la ley. Toda persona tiene derecho a acceder a los datos recogidos que la conciernan y a su rectificación.*
- 3. El respeto de estas normas quedará sujeto al control de una autoridad independiente.*

• Propiedad Intelectual e Industrial

Los derechos de propiedad intelectual se encuentran regulados por convenios internacionales auspiciados por la Organización Mundial del Comercio y la Organización Mundial de la Propiedad Intelectual (ver apartado i). Además, siguen estando más protegidos por las leyes nacionales que por la normativa comunitaria.

En el año 2001 se aprobó la polémica **Directiva de la Unión Europea sobre derecho de autor**, que adopta y adapta el Tratado de la OMPI sobre Derecho de Autor de 1996 al ámbito comunitario. Sin embargo, dado que cada estado miembro de la Unión Europea debe trasponer la directiva, con todo lo que ello implica en cuanto a coste, diferentes interpretaciones de una misma norma y adaptación a cada una de las legislaciones nacionales, sería deseable un mayor grado de armonización. No olvidemos que una directiva es un instrumento de armonización, que establece directrices esenciales, pero que otorga un gran margen de actuación y de decisión de cada estado miembro, con lo que se puede producir divergencias dando como resultado normas nacionales muy diferentes e incluso contradictorias, lo que no es deseable dado el marcado carácter transnacional de la protección de datos y demás derechos de propiedad industrial e intelectual.

iii. Legislación española

1. Ley Orgánica de Protección de Datos

La Ley Orgánica 15/1999 sobre la Protección de Datos de Carácter Personal (LOPD) que fue publicada el 14 de Diciembre de 1999 en el número 298/1999 del BOE, establece una serie de obligaciones para las empresas, los profesionales autónomos y las administraciones públicas que sean titulares de datos de carácter personal.

La LOPD tiene tres antecedentes normativos. El primero de ellos es el artículo 18 de la Constitución Española, que como podemos ver a continuación “garantiza [...] la intimidad personal y familiar” y establece que “la Ley limitará el uso de la informática para garantizar el honor y la intimidad”. Por tanto, nos encontramos ante un derecho fundamental que debe ser regulado mediante ley orgánica.

Constitución Española.

Artículo 18.

- 1. Se garantiza el derecho al honor, a la intimidad personal y familiar y a la propia imagen.*
- 2. El domicilio es inviolable. Ninguna entrada o registro podrá hacerse en el sin consentimiento del titular o resolución judicial, salvo en caso de flagrante delito.*
- 3. Se garantiza el secreto de las comunicaciones y, en especial, de las postales, telegráficas y telefónicas, salvo resolución judicial.*
- 4. La Ley limitará el uso de la informática para garantizar el honor y la intimidad personal y familiar de los ciudadanos y el pleno ejercicio de sus derechos.*

Es importante puntualizar que el artículo 55 de la Constitución Española considera situaciones bajo las cuales se podrá dejar de aplicar el artículo 18, esto es, que los derechos reconocidos en dicho artículo “podrán ser suspendidos cuando se acuerde la declaración del estado de excepción o de sitio en los términos previstos en la Constitución”.

En 1992 nace la primera ley española que regula de forma específica el uso de medios informáticos relativo a datos de carácter personal. Se trata de la **Ley Orgánica de Regulación del Tratamiento Automatizado de los Datos de Carácter Personal (LORTAD)**. En la actualidad se encuentra derogada, su ámbito de aplicación se circunscribía únicamente a los ficheros de carácter personal que se tratan en soportes automatizados.

Por último, en 1995 ve la luz la **Directiva Europea 95/46 CE** de 24 de octubre del Parlamento Europeo y del Consejo relativa a la protección de las personas físicas en lo que respecta al tratamiento de datos personales y a la libre circulación de estos datos. A finales de 1999, se publica la Ley Orgánica de Protección de Datos que traspone lo previsto en la nueva directiva europea. La LOPD amplía el ámbito de aplicación a todo tipo de ficheros de carácter personal, independientemente del tipo de soporte en el cual se traten (automatizados y no automatizados).

Dicha ley, que deroga la anterior LORTAD, tiene por objeto garantizar y proteger, en lo que respecta al tratamiento de los datos personales, las libertades públicas y los derechos fundamentales de las personas físicas, y especialmente de su honor e intimidad personal y familiar.

La legislación española de protección de datos es una de las más restrictivas a nivel mundial, tanto que choca con el funcionamiento y la esencia de Internet. Por este motivo, las distintas plataformas operativas a nivel internacional podrían encontrar problemas legales añadidos en nuestro país. Actividades perfectamente legales en otros estados podrían considerarse ilegales atendiendo a la aplicación de la LOPD.

A continuación analizaremos los artículos considerados más relevantes en cuanto a la regulación de las redes sociales en nuestro país. Obviaremos por tanto los relacionados con las Administraciones Públicas y, de momento, los que definen y regulan la existencia de la Agencia de Protección de Datos.

En primer lugar veremos una serie de definiciones necesarias para comprender la ley, indicadas en el artículo 3.

Ley Orgánica de Protección de Datos Personales.

Artículo 3.

A los efectos de la presente Ley Orgánica se entenderá por:

- a) **Datos de carácter personal:** cualquier información concerniente a personas físicas identificadas o identificables.*
- b) **Fichero:** todo conjunto organizado de datos de carácter personal, cualquiera que fuere la forma o modalidad de su creación, almacenamiento, organización y acceso.*
- c) **Tratamiento de datos:** operaciones y procedimientos técnicos de carácter automatizado o no, que permitan la recogida, grabación, conservación, elaboración, modificación, bloqueo y cancelación, así como las cesiones de datos que resulten de comunicaciones, consultas, interconexiones y transferencias.*
- d) **Responsable del fichero o tratamiento:** persona física o jurídica, de naturaleza pública o privada, u órgano administrativo, que decida sobre la finalidad, contenido y uso del tratamiento.*
- e) **Afectado o interesado:** persona física titular de los datos que sean objeto del tratamiento a que se refiere el apartado c) del presente artículo.*

*f) **Procedimiento de disociación:** todo tratamiento de datos personales de modo que la información que se obtenga no pueda asociarse a persona identificada o identificable.*

*g) **Encargado del tratamiento:** la persona física o jurídica, autoridad pública, servicio o cualquier otro organismo que, sólo o conjuntamente con otros, trate datos personales por cuenta del responsable del tratamiento.*

*h) **Consentimiento del interesado:** toda manifestación de voluntad, libre, inequívoca, específica e informada, mediante la que el interesado consienta el tratamiento de datos personales que le conciernen.*

*i) **Cesión o comunicación de datos:** toda revelación de datos realizada a una persona distinta del interesado.*

*j) **Fuentes accesibles al público:** aquellos ficheros cuya consulta puede ser realizada, por cualquier persona, no impedida por una norma limitativa o sin más exigencia que, en su caso, el abono de una contraprestación. Tienen la consideración de fuentes de acceso público, exclusivamente, el censo promocional, los repertorios telefónicos en los términos previstos por su normativa específica y las listas de personas pertenecientes a grupos de profesionales que contengan únicamente los datos de nombre, título, profesión, actividad, grado académico, dirección e indicación de su pertenencia al grupo. Asimismo, tienen el carácter de fuentes de acceso público los diarios y boletines oficiales y los medios de comunicación.*

Es importante conocer el ámbito de aplicación, tal y como se establece en el artículo 2. Observamos que, efectivamente, el tratamiento de los datos de carácter personal que pueda derivarse de las redes sociales se rige por la LOPD, ya que no parece que deban regirse por las disposiciones específicas de esta ley, ni corresponden al ejercicio de actividades exclusivamente personales y domésticas. En caso de tratarse de una red social con sede en otro país, al recogerse los datos mediante ordenadores españoles, se regirán también por la LOPD.

Ley Orgánica de Protección de Datos Personales.

Artículo 2. Ámbito de aplicación.

1. La presente Ley Orgánica será de aplicación a los datos de carácter personal registrados en soporte físico, que los haga susceptibles de tratamiento, y a toda modalidad de uso posterior de estos datos por los sectores público y privado.

Se regirá por la presente Ley Orgánica todo tratamiento de datos de carácter personal:

a) Cuando el tratamiento sea efectuado en territorio español en el marco de las actividades de un establecimiento del responsable del tratamiento.

c) Cuando el responsable del tratamiento no esté establecido en territorio de la Unión Europea y utilice en el tratamiento de datos medios situados en territorio español, salvo que tales medios se utilicen únicamente con fines de tránsito.

2. El régimen de protección de los datos de carácter personal que se establece en la presente Ley Orgánica no será de aplicación:

a) A los ficheros mantenidos por personas físicas en el ejercicio de actividades exclusivamente personales o domésticas.

b) A los ficheros sometidos a la normativa sobre protección de materias clasificadas.

c) A los ficheros establecidos para la investigación del terrorismo y de formas graves de delincuencia organizada.

No obstante, en estos supuestos el responsable del fichero comunicará previamente la existencia del mismo, sus características generales y su finalidad a la Agencia de Protección de Datos.

3. Se regirán por sus disposiciones específicas, y por lo especialmente previsto, en su caso, por esta Ley Orgánica los siguientes tratamientos de datos personales:

a) Los ficheros regulados por la legislación de régimen electoral.

b) Los que sirvan a fines exclusivamente estadísticos, y estén amparados por la legislación estatal o autonómica sobre la función estadística pública.

La LOPD confiere una serie de **derechos** para el usuario de Internet, y por lo tanto, para el usuario de las redes sociales. Según el artículo 5, se debe proporcionar la información pertinente a los interesados a los que se soliciten datos personales. Asimismo, el tratamiento de los datos de carácter personal requiere el consentimiento inequívoco del afectado (artículo 6). En cuanto a las valoraciones basadas en un tratamiento de datos personales, los ciudadanos tienen derecho a no verse sometidos a una decisión con efectos jurídicos, sobre ellos o que les afecte de manera significativa, y podrá impugnar los actos administrativos o decisiones privadas que impliquen una valoración de su comportamiento (artículo 13). Por último, los ciudadanos pueden ejercer su derecho de consulta, acceso, rectificación y cancelación (artículos 14 a 18) y de ser indemnizados en caso de sufrir daño o lesión en sus bienes o derechos (artículo 19).

Ley Orgánica de Protección de Datos Personales.

Artículo 5. Derecho de información en la recogida de datos.

1. Los interesados a los que se soliciten datos personales deberán ser previamente informados de modo expreso, preciso e inequívoco:

- a) De la existencia de un fichero o tratamiento de datos de carácter personal, de la finalidad de la recogida de éstos y de los destinatarios de la información.*
- b) Del carácter obligatorio o facultativo de su respuesta a las preguntas que les sean planteadas.*
- c) De las consecuencias de la obtención de los datos o de la negativa a suministrarlos.*
- d) De la posibilidad de ejercitar los derechos de acceso, rectificación, cancelación y oposición.*
- e) De la identidad y dirección del responsable del tratamiento o, en su caso, de su representante.*

Para garantizar estos derechos de los ciudadanos, esta ley también incluye ciertas **obligaciones** de los responsables de ficheros de tratamiento de datos de carácter personal. Para empezar, deben informar a los interesados de lo estipulado en el artículo 5. En este mismo se indica que, cuando el responsable del tratamiento no esté establecido en el territorio de la Unión Europea y utilice en el tratamiento de datos medios que radiquen en territorio español, deberá designar, salvo que tales medios se utilicen con fines de trámite, un representante en España, sin perjuicio de las acciones que pudieran emprenderse contra el propio responsable del tratamiento.

El responsable del fichero también tendrá que velar por la **calidad de los datos** (artículo 4). Estos deben ser adecuados, pertinentes o no excesivos en relación con el ámbito y finalidades legítimas para las que se han obtenido, no podrán usarse para finalidades distintas de aquellas para las que fueron recogidos. Deberán ser exactos y actualizados. Si son inexactos o están incompletos deben ser cancelados o sustituidos por los correctos. Serán cancelados cuando dejen de ser necesarios. No podrán ser conservados una vez que dejen de ser útiles para la función prevista, con excepción de la legislación específica prevista al efecto.

Según el artículo 9, el encargado del tratamiento deberá adoptar las medidas necesarias que garanticen la **seguridad** de los datos de carácter personal. No se registrarán datos de carácter personal en ficheros que no reúnan las condiciones que se determinen por vía reglamentaria con respecto a su integridad y seguridad y a las de los centros de tratamiento, locales, equipos, sistemas y programas. Legalmente, el profesional está obligado al **deber de secreto** (artículo 10), incluso después de haber finalizado la relación con el titular o el responsable del fichero.

La **comunicación de datos a terceros** está fuertemente regulada (artículos 12 y 13). El cedente debe obtener el consentimiento previo del interesado, siempre facilitándole la suficiente información como para conocer la finalidad a que destinarán los datos cuya comunicación se autoriza o el tipo de actividad de aquel a quien se pretende comunicar. Una vez cumplida la prestación contractual, los datos de carácter personal deberán ser destruidos o devueltos al responsable del tratamiento. En el momento en que se efectúe la primera cesión de datos, el responsable del fichero deberá informar de ello a los afectados, indicando asimismo, la finalidad del fichero, la naturaleza de los datos que han sido cedidos y el nombre y dirección del cesionario (artículo 27).

En lo referente al registro, toda persona o entidad que proceda a la **creación de ficheros de datos de carácter personal** lo notificará previamente a la Agencia de Protección de Datos, comunicando convenientemente los detalles del fichero (artículo 26). En los tratamientos con fines de publicidad y de prospección comercial, en cada comunicación que se dirija al interesado se informará del origen de los datos y de la identidad del responsable del tratamiento, así como de los derechos que le asisten (artículo 30).

Existen otras consideraciones, como los **datos especialmente protegidos** (artículos 7 y 8) referentes a ideología, religión o creencias, salvo que el afectado consienta expresamente y por escrito. Es obligatorio advertir al interesado sobre su derecho a no prestar su consentimiento. Sólo podrán recabarse datos que se refieran al origen racial, salud o vida sexual de conformidad con una ley concreta, por razones de interés general, o cuando el afectado consienta expresamente.

Según el artículo 33, no podrán realizarse transferencias de datos de carácter personal a países que no proporcionen un **nivel de protección equiparable** al que presta la ley española, salvo que, además de haberse observado lo dispuesto en la misma, se obtenga autorización previa del Director de la Agencia de Protección de Datos, que sólo podrá otorgarla si se obtienen las garantías adecuadas. Una de las excepciones que se contemplan es cuando la transferencia internacional de datos de carácter personal resulte de la aplicación de tratados o convenios internacionales en los que sea parte España.

Por último, los responsables de los ficheros y los encargados de los tratamientos de datos estarán sujetos al **régimen sancionador** establecido en la misma ley, por tanto estarán obligados a pagar a la Agencia de Protección de Datos las sanciones correspondientes a las infracciones cometidas (artículos 43 a 49). Existen una serie de conductas que se califican como infracciones leves, graves y muy graves.

Ley Orgánica de Protección de Datos Personales.

Artículo 44. Tipos de infracciones.

1. Las infracciones se calificarán como leves, graves o muy graves.

2. Son infracciones leves:

a) No atender, por motivos formales, la solicitud del interesado de rectificación o cancelación de los datos personales objeto de tratamiento cuando legalmente proceda.

b) No proporcionar la información que solicite la Agencia de Protección de Datos en el ejercicio de las competencias que tiene legalmente atribuidas, en relación con aspectos no sustantivos de la protección de datos.

c) No solicitar la inscripción del fichero de datos de carácter personal en el Registro General de Protección de Datos, cuando no sea constitutivo de infracción grave.

d) Proceder a la recogida de datos de carácter personal de los propios afectados sin proporcionarles la información que señala el artículo 5 de la presente Ley.

e) Incumplir el deber de secreto establecido en el artículo 10 de esta Ley, salvo que constituya infracción grave.

3. Son infracciones graves:

a) Proceder a la creación de ficheros de titularidad pública o iniciar la recogida de datos de carácter personal para los mismos, sin autorización de disposición general, publicada en el «Boletín Oficial del Estado» o Diario oficial correspondiente.

b) Proceder a la creación de ficheros de titularidad privada o iniciar la recogida de datos de carácter personal para los mismos con finalidades distintas de las que constituyen el objeto legítimo de la empresa o entidad.

c) Proceder a la recogida de datos de carácter personal sin recabar el consentimiento expreso de las personas afectadas, en los casos en que éste sea exigible.

d) Tratar los datos de carácter personal o usarlos posteriormente con conculcación de los principios y garantías establecidos en la presente Ley o con incumplimiento de los preceptos de protección que impongan las disposiciones reglamentarias de desarrollo, cuando no constituya infracción muy grave.

e) El impedimento o la obstaculización del ejercicio de los derechos de acceso y oposición y la negativa a facilitar la información que sea solicitada.

f) Mantener datos de carácter personal inexactos o no efectuar las rectificaciones o cancelaciones de los mismos que legalmente procedan cuando resulten afectados los derechos de las personas que la presente Ley ampara.

g) La vulneración del deber de guardar secreto sobre los datos de carácter personal incorporados a ficheros que contengan datos relativos a la comisión de infracciones administrativas o penales, Hacienda Pública, servicios financieros, prestación de servicios de solvencia patrimonial y crédito, así como aquellos otros ficheros que contengan un conjunto de datos de carácter personal suficientes para obtener una evaluación de la personalidad del individuo.

h) Mantener los ficheros, locales, programas o equipos que contengan datos de carácter personal sin las debidas condiciones de seguridad que por vía reglamentaria se determinen.

i) No remitir a la Agencia de Protección de Datos las notificaciones previstas en esta Ley o en sus disposiciones de desarrollo, así como no proporcionar en plazo a la misma cuantos documentos e informaciones deba recibir o sean requeridos por aquél a tales efectos.

j) La obstrucción al ejercicio de la función inspectora.

k) No inscribir el fichero de datos de carácter personal en el Registro General de Protección Datos, cuando haya sido requerido para ello por el Director de la Agencia de Protección de Datos.

l) Incumplir el deber de información que se establece en los artículos 5, 28 y 29 de esta Ley, cuando los datos hayan sido recabados de persona distinta del afectado.

4. Son infracciones **muy graves**:

a) La recogida de datos en forma engañosa y fraudulenta.

b) La comunicación o cesión de los datos de carácter personal, fuera de los casos en que estén permitidas.

c) Recabar y tratar los datos de carácter personal a los que se refiere el apartado 2 del artículo 7 cuando no medie el consentimiento expreso del afectado; recabar y tratar los datos referidos en el apartado 3 del artículo 7 cuando no lo disponga una ley o el afectado no haya consentido expresamente, o violentar la prohibición contenida en el apartado 4 del artículo 7.

d) No cesar en el uso ilegítimo de los tratamientos de datos de carácter personal cuando sea requerido para ello por el Director de la Agencia de Protección de Datos o por las personas titulares del derecho de acceso.

e) La transferencia temporal o definitiva de datos de carácter personal que hayan sido objeto de tratamiento o hayan sido recogidos para someterlos a dicho tratamiento, con destino a países que no proporcionen un nivel de protección equiparable sin autorización del Director de la Agencia de Protección de Datos.

f) Tratar los datos de carácter personal de forma ilegítima o con menosprecio de los principios y garantías que les sean de aplicación, cuando con ello se impida o se atente contra el ejercicio de los derechos fundamentales.

g) La vulneración del deber de guardar secreto sobre los datos de carácter personal a que hacen referencia los apartados 2 y 3 del artículo 7, así como los que hayan sido recabados para fines policiales sin consentimiento de las personas afectadas.

h) No atender, u obstaculizar de forma sistemática el ejercicio de los derechos de acceso, rectificación, cancelación u oposición.

i) No atender de forma sistemática el deber legal de notificación de la inclusión de datos de carácter personal en un fichero.

Agencia Española de Protección de Datos

La Agencia Española de Protección de Datos (AEPD) es la autoridad de control independiente que vela por el cumplimiento de la normativa sobre protección de datos y garantiza y tutela el derecho fundamental a la protección de datos de carácter personal en España. Es un ente de Derecho Público, con personalidad jurídica propia y plena capacidad pública y privada. Actúa con independencia de las Administraciones Públicas en el ejercicio de sus funciones, tal y como establece el artículo 8 de la Carta de los Derechos Fundamentales de la Unión Europea.

Son funciones de la AEPD:

1. Atender las peticiones y reclamaciones presentadas por los afectados.
2. Proporcionar información acerca de sus derechos.
3. Ejercer la potestad sancionadora, en los términos previstos en la ley.
4. Ordenar el cese o inmovilización de los ficheros que proceda.
5. Inspeccionar los ficheros, recabando cuantas informaciones se precisen para el cumplimiento de sus cometidos.

6. Ejercer el control y adoptar las autorizaciones que procedan en relación a los movimientos internacionales de datos.

La AEPD establece relaciones con los representantes de diversas redes sociales para discutir sobre el aspecto de la privacidad, y no duda en criticar los fallos y cambios propuestos si los consideran poco seguros para el usuario.

2. Ley de Propiedad Intelectual

En España, la Propiedad Intelectual está regulada en la Ley de Propiedad Intelectual de 1996 (modificada por la Ley 23/2006, de 7 de julio), siendo parte dicha ley de nuestro Derecho Civil. Esta ley protege las obras originales y creaciones artísticas, literarias o científicas.

Del mismo modo que en el apartado anterior sobre la Protección de Datos, recopilaremos los artículos susceptibles de entrar en conflicto con las prácticas llevadas a cabo en las redes sociales.

Existen unos derechos morales, irrenunciables para el autor, y unos derechos de explotación que sí se pueden ceder. El artículo 14 incluido a continuación versa sobre los derechos morales.

Artículo 14. Contenido y características del derecho moral

Corresponden al autor los siguientes derechos irrenunciables e inalienables:

1. Decidir si su obra ha de ser divulgada y en qué forma.
2. Determinar si tal divulgación ha de hacerse con su nombre, bajo seudónimo o signo, o anónimamente.
3. Exigir el reconocimiento de su condición de autor de la obra.
4. Exigir el respeto a la integridad de la obra e impedir cualquier deformación, modificación, alteración o atentado contra ella que suponga perjuicio a sus legítimos intereses o menoscabo a su reputación.
5. Modificar la obra respetando los derechos adquiridos por terceros y las exigencias de protección de bienes de interés cultural.

6. Retirar la obra del comercio, por cambio de sus convicciones intelectuales o morales, previa indemnización de daños y perjuicios a los titulares de derechos de explotación.

Si, posteriormente, el autor decide reemprender la explotación de su obra deberá ofrecer preferentemente los correspondientes derechos al anterior titular de los mismos y en condiciones razonablemente similares a las originarias.

7. Acceder al ejemplar único o raro de la obra, cuando se halle en poder de otro, a fin de ejercitar el derecho de divulgación o cualquier otro que le corresponda.

Este derecho no permitirá exigir el desplazamiento de la obra y el acceso a la misma se llevará a efecto en el lugar y forma que ocasionen menos incomodidades al poseedor, al que se indemnizará, en su caso, por los daños y perjuicios que se le irroguen.

Respecto a los derechos patrimoniales, indica la Ley que “corresponde al autor el ejercicio exclusivo de los derechos de explotación de su obra en cualquier forma y, en especial, los derechos de reproducción, distribución, comunicación pública y transformación, que no podrán ser realizadas sin su autorización, salvo en los casos previstos en la presente Ley” (artículo 17).

Los derechos patrimoniales se mantendrán cuando el autor sea una persona física, durante toda su vida, y después de su muerte o declaración de fallecimiento. Cuando el autor sea una persona jurídica, la duración de los derechos patrimoniales se mantendrá durante los 50 años siguientes a su lícita divulgación o, caso de no haberse divulgado, al momento de su creación. Normalmente, para evitar malentendidos los 50 años comienzan a contarse a partir del 1 de enero siguiente. Los derechos patrimoniales incluyen la reproducción, distribución, comunicación pública y transformación (artículos 18 a 21 de la LPI).

- **Derecho de reproducción**

Se entiende por reproducción la fijación directa o indirecta, provisional o permanente, por cualquier medio y en cualquier forma, de toda la obra o de parte de ella, que permita su comunicación o la obtención de copias.

- **Derecho de distribución**

Se entiende por distribución la puesta a disposición del público del original o de las copias de la obra, en un soporte tangible, mediante su venta, alquiler, préstamo o de cualquier otra forma.

- **Derecho de comunicación pública**

Se entenderá por comunicación pública todo acto por el cual una pluralidad de personas pueda tener acceso a la obra sin previa distribución de ejemplares a cada una de ellas.

No se considerará pública la comunicación cuando se celebre dentro de un ámbito estrictamente doméstico que no esté integrado o conectado a una red de difusión de cualquier tipo.

- **Derecho de transformación**

La transformación de una obra comprende su traducción, adaptación y cualquier otra modificación en su forma de la que se derive una obra diferente.

Los derechos de propiedad intelectual de la obra resultado de la transformación corresponderán al autor de esta última, sin perjuicio del derecho del autor de la obra preexistente de autorizar, durante todo el plazo de protección de sus derechos sobre ésta, la explotación de esos resultados en cualquier forma y en especial mediante su reproducción, distribución, comunicación pública o nueva transformación.

El usuario a su vez goza de ciertos derechos, estipulados en el capítulo II (Límites). Se puede resumir en cuatro excepciones: las reproducciones provisionales, la copia privada, la cita y la parodia.

Para cerrar este apartado sobre la LPI española, comentaremos los cambios establecidos en la ley 23/2006, que ofrece a los autores una compensación equitativa por copia privada, o también conocido como Canon Digital.

Artículo 25. *Compensación equitativa por copia privada*

1. La reproducción realizada exclusivamente para uso privado, mediante aparatos o instrumentos técnicos no tipográficos, de obras divulgadas en forma de libros o publicaciones que a estos efectos se asimilen reglamentariamente, así como de fonogramas, videogramas o de otros soportes sonoros, visuales o audiovisuales, originará una compensación equitativa y única por cada una de las tres modalidades de reproducción mencionadas, en favor de las personas que se expresan en el párrafo b) del apartado 4, dirigida a compensar los derechos de propiedad intelectual que se dejaron de percibir por razón de la expresada reproducción. Este derecho será irrenunciable para los autores y los artistas, intérpretes o ejecutantes.

2. Esa compensación se determinará para cada modalidad en función de los equipos, aparatos y soportes materiales idóneos para realizar dicha reproducción, fabricados en territorio español o adquiridos fuera de éste para su distribución comercial o utilización dentro de dicho territorio.

Es evidente que en el contexto de las redes sociales, el canon digital carece de sentido. Las reproducciones ya no se albergan en soportes físicos tales como CD, DVD, discos duros... sino en los servidores de las distintas páginas web, ubicados generalmente fuera de España, y por tanto exentos de pagar dicha compensación a los artistas.

3. Ley de Propiedad Industrial

Los derechos de propiedad industrial son privilegios absolutos o de exclusión que solamente se adquieren mediante la inscripción en un registro especial de la propiedad. En España, la Oficina Española de Patentes y Marcas (OEPM) protege las distintas modalidades de propiedad industrial.

Hay dos modalidades de propiedad industrial:

1. Los signos distintivos del empresario (autónomo o persona jurídica), el establecimiento y los productos o servicios (el nombre comercial y las marcas), que se protegen porque permiten su distinción respecto a los demás. Las marcas permiten a su titular distinguir su producto de cualquier otro, aunque sea de la misma naturaleza, de modo que alguno productos acaban denominándose con el nombre de la marca (por ejemplo, “Coca-Cola” es la marca de un refresco de cola, y “Kodak” de fotografía).

2. Por otro lado, las patentes, modelos de utilidad, dibujos industriales y artísticos, (ver glosario) que son susceptibles de protección como creaciones intelectuales porque aportan soluciones a problemas tecnológicos o de diseño y tienen una amplia proyección en el terreno económico.¹⁸ Son susceptibles de protección aquellos inventos que sean **novedosos**, por lo que la patente protege sobre todo una idea que se plasma a través de diseños, modelos o dibujos que se registran para que nadie pueda reivindicar la autoría de los mismos, y por tanto, para poder explotarlos económicamente.

Debido a esto, los usuarios no podrán subir contenido que incluya signos distintivos protegidos ni creaciones intelectuales, industriales y artísticas susceptibles de protección.

¹⁸ El Exportador Digital (revista Digital del ICEX). Marzo 2003.

b. Contrato de adhesión

Todas las redes sociales tienen unos términos y condiciones de uso que el usuario debe aceptar antes de poder crear su propia cuenta. No obstante, la gran mayoría de los usuarios no leen estos términos, por lo que desconocen completamente a qué riesgos se exponen. Como curiosidad, comentaremos una noticia que refleja este hecho. La empresa británica de videojuegos GameStation ha anunciado que posee las almas de cerca de 7.500 clientes que aceptaron los términos y condiciones legales de sus productos en venta en su tienda online, gracias a una cláusula legal que, como vaticinaron, nadie leyó¹⁹. Los resultados de la “broma” son bastante alarmantes: más del 88% de los usuarios no leen los términos legales.

i. Facebook

Esta red social ofrece una **Declaración de derechos y responsabilidades**²⁰ así como una serie de documentos para consulta del usuario: Política de Privacidad, Términos de de Pago, Acerca de la plataforma, Principios y políticas para los desarrolladores, Normas de Publicidad, Normas de promoción y Términos de las páginas. Asimismo ayuda a denunciar posibles infracciones de los derechos de propiedad intelectual.

Facebook establece diez principios como fundamento de los derechos y responsabilidades de aquellos que conforman el servicio de su red social²¹

Principios de Facebook

1. Libertad para compartir y conectarse

Las personas deben disfrutar de la libertad de compartir cualquier información que deseen, a través de cualquier medio y formato, y tener el derecho de poder conectarse en línea con otros (personas, organizaciones o servicios) siempre que ambas partes consientan la conexión.

2. Propiedad y control de la información

Las personas deben ser propietarias de su información. Deben tener libertad para compartirla con cualquiera que ellos decidan, llevarla consigo a cualquier lugar e incluso retirarla del servicio de Facebook. Las personas deben tener libertad para decidir con quién quieren compartir su información y para establecer los controles de privacidad que protejan sus decisiones. Estos controles, no obstante, no pueden limitar el modo en el que aquellos que reciben la información la utilizan, especialmente si esto ocurre fuera del servicio de Facebook.

¹⁹ <http://www.elmundo.es/mundodinero/2010/04/20/economia/1271784338.html>

²⁰ <http://www.facebook.com/terms.php>

²¹ <http://www.facebook.com/principles.php>

3. Flujo libre de información

Las personas deben tener libertad de acceso a toda la información que otros pongan a su disposición. Las personas también deben disponer de las herramientas prácticas para que compartir la información y acceder a ella resulte más fácil, rápido y eficaz.

3. Igualdad fundamental

Toda persona (ya sea un individuo, anunciante, desarrollador, organización u otra entidad) debe tener representación y acceso a la distribución e información dentro del servicio de Facebook, independientemente de la actividad principal de dicha persona. Debe existir un conjunto único de principios, derechos y responsabilidades que se apliquen a todas las personas que utilicen el servicio de Facebook.

4. Valor social

Las personas deben tener libertad para forjarse confianza y reputación a través de su identidad y sus conexiones, y no deben ser retiradas del servicio de Facebook por razones diferentes de las descritas en la Declaración de derechos y responsabilidades de Facebook.

5. Plataformas y estándares abiertos

Las personas deben contar con interfaces programáticas para compartir y acceder a la información que se pone a su disposición. Las especificaciones para estas interfaces deben publicarse y ser accesibles para todos.

6. Servicio fundamental

Las personas deben ser capaces de utilizar Facebook de forma gratuita para establecer una presencia, conectarse con otros y compartir información con ellos. Toda persona tiene que poder utilizar el servicio de Facebook, independientemente de su nivel de participación o contribución.

7. Bienestar común

Los derechos y responsabilidades de Facebook y de las personas que lo utilizan deben describirse en una Declaración de derechos y responsabilidades, que tiene que ser coherente con estos principios.

8. Proceso transparente

Facebook debe publicar la información acerca de su propósito, planes, políticas y operaciones. Facebook debe tener un procedimiento de notificaciones y comentarios, así como un sistema de votos, que fomenten la participación y el debate sobre las modificaciones de estos principios o los derechos y responsabilidades.

9. Un mundo

El servicio de Facebook debe traspasar las barreras nacionales y geográficas y estar disponible para todo el mundo.

1. Privacidad

Facebook es titular de una licencia de certificación del **programa de privacidad TRUSTe**. Esta organización independiente lleva el programa de garantía de privacidad más importante del mundo. Certifica a más de 3.500 páginas web, entre las cuales se encuentran portales y marcas como Yahoo, Microsoft, Apple Inc., IBM, Oracle, Intuit, eBay y, como ya hemos mencionado, Facebook. Además de sus certificaciones de privacidad, TRUSTe ofrece servicios profesionales como la gestión de la reputación, creación de una política de privacidad, evaluación del vendedor y resolución de disputas sobre la privacidad del consumidor.

Facebook también participa en el marco **Safe Harbor** (Puerto Seguro, ver apartado 3.a.i.) desarrollado por el Departamento de Comercio de Estados Unidos y la Unión Europea. De este modo se consigue un nivel de seguridad y privacidad satisfactorio para gran cantidad de países, y se permite la transferencia de datos entre diferentes regiones, ya que al utilizar Facebook el usuario da su consentimiento para que los datos personales sean transferidos y procesados en Estados Unidos.

Los **menores** reciben un tratamiento especial. Para empezar, no se acepta información de niños menores de 13 años, y en el caso concreto de España, menores de 14 años. Facebook se reserva el derecho de aplicar métodos de protección especial, como proporcionarles un contenido adecuado a su edad, y aplicar restricciones a la capacidad que tienen los adultos para compartir contenidos y conectarse a menores. Asimismo, se recomienda encarecidamente que los menores de 13 años o más pidan permiso a sus padres antes de enviar información sobre sí mismos, y se anima a los padres a que enseñen a sus hijos prácticas seguras para el uso de Internet.

En cuanto a la información enviada, se debe facilitar un nombre (verdadero), correo electrónico, sexo y fecha de nacimiento. De manera opcional uno puede conectarse a las redes que le interesen (amigos, centros educativos, actividades...) así como información personal, como tendencias políticas y religiosas. Cabe destacar que estos son considerados **datos especialmente protegidos** en la LOPD, y que por tanto se debería advertir al interesado su derecho a no prestar su consentimiento. Sin embargo, en ningún momento se le avisa. El nombre y la fotografía carecen de configuración de privacidad, pero para el resto de información, así como para las publicaciones, el usuario puede seleccionar una configuración determinada.

Facebook almacena información sobre cada usuario. Además del contenido que se sube, como es obvio, se guardan los datos sobre transacciones o pagos realizados a través de la plataforma, además de información de amigos mediante la Herramienta de Importación de Contactos. En cualquier momento el usuario puede solicitar que se eliminen estos datos. A través de la interacción del usuario, se realiza un seguimiento de las acciones realizadas, y se almacena información sobre el dispositivo y navegador desde el que se accede (cookies).

La información se puede obtener de terceros. Las aplicaciones o sitios web que se usan a través de la plataforma no son propiedad de Facebook. Tras aceptar una serie de condiciones que limitan el uso de la información (conforme con el artículo 12 de la LOPD). Facebook puede solicitar información de cómo los usuarios responden a los

anuncios para medir la efectividad de la publicidad. También se puede obtener información a partir de otros usuarios (si un amigo etiqueta una foto, por ejemplo).

El usuario deberá tener especial cuidado cuando tenga su configuración de privacidad establecida en “Todos”. En esta modalidad, la información permanece accesible y visible para todo aquel que entre en Internet (incluidas las personas no registradas en Facebook), y queda sujeta a la indexación por parte de motores de búsqueda de terceros y puede ser importada, exportada, distribuida y redistribuida por Facebook y otros sin limitaciones de privacidad. La configuración predeterminada en Facebook es “todos”. Aunque el usuario cambie más tarde su configuración, ya no hay manera de controlar el uso de su información fuera de Facebook.

Cuando se desactiva una cuenta, ningún usuario puede verla, pero no será eliminada. Por el contrario, cuando se elimina una cuenta, se borra de forma permanente de Facebook. Esta cláusula es relativamente nueva, ya que con anterioridad Facebook se apropiaba de esos datos de forma indefinida. Sin embargo, pueden permanecer copias de dicha información en la medida en que se haya compartido con otros, y Facebook puede conservar cierta información para evitar el robo de identidades

Para responder a requerimientos legales y evitar daños, Facebook puede revelar información con arreglo a citaciones, órdenes judiciales u otros requerimientos si lo exige la ley. En el caso de España, este acto se vería limitado por el artículo 13 de la LOPD.

Por último, se toman medidas para mantener la información a salvo, como dispone la ley. La información se almacena en un servidor protegido con un firewall, y la información confidencial es cifrada usando la tecnología de capa de socket seguro (SSL). Sin embargo Facebook informa de que ninguna medida de seguridad es perfecta ni impenetrable, por tanto no pueden garantizar la seguridad en Facebook.

2. Propiedad Intelectual

El usuario es (o debe ser) propietario de todo el contenido y la información que publica en Facebook. Para el contenido protegido por derechos de propiedad intelectual, se concede una licencia exclusiva, transferible, con posibilidad de ser sub-otorgada, sin royalties, aplicable globalmente, para utilizar cualquier contenido de PI que se publique en Facebook. También es importante señalar que la LPI establece que la cesión de derechos a terceros debe ser expresa, es decir, que por defecto, la cesión a terceros está prohibida y requiere el consentimiento claro y expreso del titular de esos derechos. De hecho la LPI en su art. 45 exige la formalización por escrito de cualquier cesión de derechos. Esta licencia finaliza cuando se elimina el contenido o la cuenta, salvo si el contenido se ha compartido con terceros y éstos no lo han eliminado.

Igualmente, cuando el usuario elimina contenido de PI, se borra en un tiempo razonable (cuando se borre de las copias de seguridad, donde no estará disponible para terceros). Es necesario reseñar que la LPI española establece que una cesión de derechos de propiedad intelectual debe conllevar un ámbito geográfico en el que se aplicaría (en este caso, parece que se trata de todo el mundo) y, lo más importante, un ámbito temporal, es decir un plazo. Es más, la LPI establece para plazos de explotación para cada tipo de obra (colectiva, en colaboración, anónima, etc.) en sus art. 26 y siguientes.

La LPI establece igualmente que en la transmisión inter vivos de los derechos de autor, “a falta de mención del tiempo limita la transmisión a cinco años y la del ámbito territorial al país en el que se realice la cesión”, por lo que sería conveniente tener en cuenta esta disposición a la hora de ceder nuestros derechos a Facebook.

Por otra parte, Facebook proporciona las herramientas necesarias para ayudar a los usuarios a proteger los derechos de Propiedad Intelectual. Está explícitamente prohibido en los Términos publicar contenido que infrinja o viole los derechos de otros o que viole la ley de algún modo. Sin embargo, y dado que Facebook existe en todo el mundo, no queda del todo claro qué ley sería de aplicación.

3. Fines comerciales y publicidad

Está prohibido publicar comunicaciones comerciales no autorizadas, del mismo modo que no se puede usar el nombre de una marca comercial registrada si el propietario la reclama.

Facebook tiene el compromiso de mantener el sitio despejado, coherente y libre de publicidad engañosa. Para eso ha establecido una serie de normas que se aplican a todos los anuncios, sin embargo en la práctica no se controla con rigor. Por ejemplo, la regla 6 sobre las URL de destino establece que “los anuncios no deben instar a los usuarios a hacer clic en el anuncio para enviar información que los pueda identificar”. Sin embargo esto es exactamente lo que realiza una escuela de negocios en su publicidad.

4. Disposiciones aplicables a desarrolladores

El desarrollador es responsable de su aplicación, su contenido y del uso de la plataforma. Sólo solicitará la información necesaria, la cual se indicará de manera explícita a los datos, y les permitirá el derecho de eliminación de la aplicación así como de sus datos. Está prohibido hacer publicidad y transmitir esa información a terceros.

5. Conflictos

Las leyes del estado de California rigen la declaración de Derechos y Responsabilidades. Cualquier demanda se resolverá en un tribunal estatal o federal del condado de Santa Clara.

Si alguien interpone una demanda contra Facebook relacionada con las acciones, el contenido o la información de un tercero, éste se encargará de indemnizar a Facebook y les librará de la responsabilidad por todos los posibles daños, pérdidas y gastos de cualquier tipo relacionados con dicha demanda.

ii. Tuenti

1. Privacidad

La recogida y tratamiento de datos personales así como el ejercicio de derechos sobre dichos datos en Tuenti se rigen por unas Condiciones de uso²² y la Política de Privacidad y Protección de Datos. Veremos que coincide en la mayoría de los aspectos tratados con Facebook y otras redes sociales.

Se puede afirmar que Tuenti tiene una política respecto a los menores todavía más restrictiva. Se hace hincapié en los Términos de que el acceso al servicio está prohibido a los menores de 14 años, y se avisa que el equipo de Tuenti puede ponerse en contacto con el usuario para comprobar su edad mediante un documento de identidad. También se recomienda a los menores que informen y consulten con sus padres o tutores legales a la hora de transmitir información a terceros.

Tuenti ofrece una serie de funcionalidades diferentes de otras redes sociales. **Tuenti Páginas** permite a los usuarios interactuar alrededor de sus intereses, actividades y preferencias. Aquí sí encontraremos instituciones, marcas comerciales, ONGs y similares. **Tuenti Sitios** permite compartir opiniones y contenidos sobre sitios de ocio tales como restaurantes, bares, comercios, pubs, museos...

La plataforma no censura ningún tipo de opinión, siempre y cuando sea respetuosa y educada. Un servicio polémico ofrecido por Tuenti Sitios es **Tuenti Checkin**. Con este servicio, los usuarios de Tuenti podrán determinar su localización mediante dispositivos móviles para poder contactar con sus amigos así como para compartir opiniones y reseñas de los “sitios” que están visitando. Tuenti no hará seguimiento de la información de geo-localización.

Otra funcionalidad que ofrece Tuenti a sus usuarios es Tuenti Juegos. Los Juegos son provistos por terceras personas, luego los usuarios que soliciten los servicios de juegos permitirán a Juegos el acceso a su información. Tuenti le comunicará y/o permitirá el acceso a Metrogames US Inc. a la información de perfil, fotografías y cualquier otro contenido que se necesite para el funcionamiento de las aplicaciones. Los usuarios, al registrarse, consienten de manera expresa el acceso a su información.

Esta plataforma también permite la creación de eventos. Un usuario puede crear su propio evento o inscribirse a un evento, ya sea creado por otro amigo o patrocinado (de una empresa con la que Tuenti colabora).

Queda prohibido insertar en una web, blog, foro o perfil de Tuenti o de cualquier red social un vínculo que redirija a URLs de contenidos de Tuenti. Asimismo, no se permite la suplantación de personalidad, aunque se haya otorgado permiso.

A Tuenti se accede a través de invitación, para garantizar que un nuevo usuario tenga acceso a al menos una red nada más llegar. El amigo tendrá que aceptar la invitación y cumplir con el proceso de registro.

²² http://www.tuenti.com/#m=Terms&func=view_terms_of_use

Existen tres niveles de privacidad: sólo mis amigos, sólo hasta amigos de mis amigos y todos. Igualmente se puede configurar de forma específica quién tiene acceso al tablón, a los números de teléfono, a las fotos... y además se pueden bloquear a usuarios y fotos no deseados.

En cuanto a la baja de una cuenta, en los términos se explica que el usuario “no podrá volver a entrar con la misma cuenta y perderá toda la información personal, incluida las fotos, que aparecen en el perfil”. Llama la atención que no se menciona la futura utilización de los datos por parte de Tuenti, si serán eliminados o no. En el apartado Tratamiento de Datos Personales y Publicidad se comenta que Tuenti ha informado a la Agencia de Protección de Datos, y que el usuario tiene derecho de acceso a poder acceder a sus datos personales para saber cómo y con qué finalidad se tratan, así como derecho de oposición, rectificación y cancelación.

2. Propiedad Intelectual

Tuenti, como propietario del Servicio, concede al usuario una licencia limitada, revocable y no sub-licenciable para usar el Servicio de forma estrictamente personal. Está prohibido cualquier acto de explotación de la totalidad o parte de los contenidos que integran el sitio web. Por otro lado, el usuario conserva todos sus derechos sobre los contenidos publicados en su perfil. Otorgará a Tuenti una licencia limitada, mundial y no exclusiva para reproducir y comunicar públicamente los mismos, por todo el tiempo que esté vigente el perfil. Una vez se elimine el contenido o se dé de baja el perfil, se interrumpirá la comunicación del contenido. Existe una herramienta en la plataforma para notificar la infracción de derechos de autor.

Entendemos que la cesión de derechos en este caso se ajusta más a la LPI que la de Facebook, ya que no se permite la cesión a terceros (no se permite la sub-licencia) lo que permite al usuario mantener el control de sus datos y de su información y saber quién dispone de qué; la licencia no es exclusiva y además parece que se deduce un plazo (“el tiempo de vigencia del perfil”) aunque sería aconsejable especificar más claramente el plazo de la licencia.

3. Fines comerciales y publicidad

Salvo las herramientas publicitarias, los servicios se ofrecen para uso personal y las personas jurídicas tienen prohibido tener un perfil. Asimismo, no se puede suministrar datos falsos, y el usuario tiene la obligación de mantenerlos actualizados. El usuario se compromete a hacer un uso correcto del servicio, sujeto a las condiciones y a la legalidad vigente. Tuenti actúa como mero intermediario: hará todo lo razonablemente posible para vigilar la legalidad de los contenidos, pero el control absoluto de éstos es imposible.

4. Conflictos

La normativa vigente determinará las leyes que deben regir y la jurisdicción que deba conocer de las relaciones entre Tuenti y los usuarios del sitio web. No obstante, en caso de conflicto, Tuenti y el usuario se someterían a los Juzgados y Tribunales de la ciudad de Madrid. Esta opción de fuero nacional es mucho mejor para los usuarios españoles ya que es más probable que conozcan el Derecho y el sistema jurisdiccional español que el aplicable en Estados Unidos.

iii. Twitter

1. Privacidad

Al utilizar los servicios de Twitter, el usuario accede a la recogida, almacenamiento, divulgación o uso de su información, tal y como se estipula en la política de privacidad²³ en los Estados Unidos y en cualquier otro país en el que Twitter opere.

Cuando el usuario se registra, se le pide una cantidad limitada de información: nombre, nombre de usuario, contraseña y dirección de correo electrónico. El nombre y el nombre de usuario se mostrarán públicamente en el perfil de usuario. El usuario puede proporcionar información adicional como una biografía, una imagen... de forma totalmente opcional.

En cuanto se envía un Tweet, Twitter considera que el usuario le está pidiendo que haga pública esa información. Además de publicarlo, permite que la gente lo pueda buscar, lo pone a disposición de los usuarios vía SMS y lo comparte con una amplia variedad de desarrolladores y servicios. También son públicas por defecto las listas que el usuario crea, la gente a la que sigue y los tweets marcados como favoritos. En el área de configuración, se puede seleccionar la opción “Proteger mis Tweets”, para que los tweets no estén disponibles públicamente. De manera opcional se puede publicar información acerca de la localización geográfica.

Igualmente, Twitter almacena información de los enlaces publicados en los Tweets, para ayudar a mejorar sus servicios. Como muchos sitios, Twitter utiliza la tecnología Cookie para recoger datos adicionales con el mismo fin.

En cuanto a los servicios ofrecidos por terceros, Twitter permite que se recolecte información enviada por el navegador como parte de un requerimiento de la página web, tal como cookies o la dirección IP. Asimismo, Twitter comparte esta información con proveedores de servicios. Twitter considera información no-privada o no-personal los Tweets públicos y el número de usuarios que hacen clic sobre un vínculo concreto, por lo que se reserva el derecho de compartir esta información.

²³ <https://twitter.com/tos>

Como en las demás redes sociales, existe un límite de edad para el uso de los servicios, en este caso ligeramente menos restrictivo, ya que es a partir de los 13 años para todos los países.

2. Propiedad Intelectual

El usuario se reserva los derechos de cualquier contenido enviado, publicado o presentado a través de los Servicios. Al enviar, publicar o presentar cualquier Contenido a través de estos Servicios, el usuario otorga a Twitter licencia mundial, no exclusiva, libre de royalties (con derecho a la concesión de la licencia a terceros) para utilizar, copiar, reproducir, procesar, adaptar, modificar, publicar, transmitir, mostrar y distribuir dicho Contenido cualquier medio de comunicación o método de distribución (actual o desarrollado en un futuro). Observamos de nuevo que se puede ceder a terceros cualquier información, por lo que es más fácil perder la pista de quién puede ostentar finalmente nuestros derechos. A pesar de que al LPI exige un consentimiento expreso, por escrito, de cada cesión, en este caso, la cesión se produce desde el primer momento.

3. Fines comerciales y publicidad

Twitter utiliza información de los usuarios para ofrecerles publicidad adaptada a sus intereses. Por ejemplo, extrae información de sus Tweets, los Tweets que sigue, el número de clics a anunciantes...

4. Desarrolladores de API

Twitter posee una normativa que informa de cómo los desarrolladores de API pueden interactuar con el contenido de los usuarios. A grandes rasgos, se guían por cuatro principios: no sorprender a los usuarios (Mantener la integridad de los Tweets, obtener los permisos necesario del usuario en cuanto a privacidad se refiere), no hacer o distribuir Spam, respetar la privacidad del usuario y ser un buen socio de Twitter (básicamente respetar ciertas normas).

5. Ley aplicable y jurisdicción correspondiente

Estas Condiciones o cualquier otra acción relativa a ellas estarán regidas por las leyes del Estado de California sin tener en cuenta o aplicación las cláusulas de Conflicto de leyes del estado o país de residencia del usuario.

c. Derechos potencialmente vulnerables

i. Derecho al Honor

Las redes sociales pueden suponer un nuevo instrumento para perpetrar delitos contra el honor y la imagen personal de un usuario. Primero veremos cuáles son los delitos contra el honor: el delito de calumnia y el de injuria.

Incurre en un delito de **calumnia** la persona que acusa a otra de haber cometido un delito a sabiendas de que tal acusación es falsa. Tanto el delito como la persona a la que se le imputa su comisión han de estar determinados. Si el acusado de un delito de calumnia logra acreditar que los hechos que se le atribuyen a la persona supuestamente calumniada son ciertos, quedará exento de toda responsabilidad penal.

La **injuria** es aquella expresión que lesiona la dignidad de una persona perjudicando su reputación o atentando contra su propia estima. Puede consistir en la atribución de unos hechos, en formular juicios de valor sobre ella... etc. Únicamente son constitutivas de delito las injurias consideradas socialmente de carácter grave.

En este nuevo entorno resulta muy fácil atentar contra el honor de una persona, y lo que es más grave, de forma pública. Basta con una publicación en el muro (en el propio o en el de la persona afectada), un cambio de estado o un Tweet para destrozar la reputación de una persona. Estos delitos están tipificados en el Código Penal y por tanto están penados por la ley. En las redes sociales en principio la identidad de los usuarios es bastante visible, contrariamente a otros medios como foros de discusión o prensa donde se puede firmar con un pseudónimo. Por tanto sería más fácil conocer el autor de las injurias y calumnias, a no ser que haya utilizado datos falsos, lo cual está prohibido en las redes sociales.

ii. Intimidad Personal y Familiar

El derecho a la intimidad personal y familiar, establecido en el artículo 18 de la constitución española, es más vulnerable que nunca. La jurisprudencia ha entendido esta garantía fundamental como la facultad que implica “exigir de los demás el respeto de un ámbito exclusivo que incumbe solamente al individuo, que es resguardo de sus posesiones privadas, de sus propios gustos y de aquellas conductas o actitudes personalísimas que no está dispuesto a exhibir, y en el que no caben legítimamente las intromisiones externas.”

Es evidente que las redes sociales no son un ámbito exclusivo. Sin embargo la información que incluye sí puede ser privada, y será responsabilidad del usuario afectado y del buen juicio de sus amigos de su red el publicar algo en el muro o por mensaje, por ejemplo. Aunque una persona no esté dispuesta a exhibir sus gustos y las conductas o actitudes personales, es muy fácil que por unas líneas en el muro o la publicación de una foto por parte de un amigo de forma inconsciente acarree problemas. No hay que olvidar, que por mucho que se restrinja el círculo en las redes sociales (se seleccione “sólo amigos” en la configuración de privacidad), no existe garantía alguna

de que los datos no salgan del ámbito especificado. Por el mero hecho de que una persona que no deseamos acceda a nuestra información se haga “amiga” de un amigo nuestro, tendrá acceso a contenidos nuestros publicados en el muro de dicho amigo.

Es necesario señalar que no es necesario que la información tenga un contenido “sensible”; basta con colgar una foto de una comida familiar o de una fiesta de cumpleaños, que son situaciones que pertenecen al ámbito estrictamente íntimo, sin tener el consentimiento de todos los que aparecen en la foto, para infringir ese derecho. No es suficiente con etiquetar, sino que el derecho a la propia imagen implica que los titulares tienen el derecho de oponerse a la publicación de unas fotos en las que aparezcamos, siempre que no estemos en un lugar público (esto es especialmente importante cuando hablamos de personajes famosos).

En lo referente a los menores, la Ley 1/1982 de Protección Civil del Derecho al Honor, a la Intimidad Personal y Familiar y a la Propia Imagen exige, con el objetivo de defender los intereses de los menores de edad, que sus representantes legales sean los que autoricen por escrito cualquier publicación de su imagen, incluyendo en Internet, debiendo notificar dicha publicación a la Fiscalía de Menores (artículo 3.2). Obviamente esta ley no se respeta en ninguna de las plataformas, dado que la edad mínima para participar es de 13 ó 14 años.

iii. Derecho a la propia imagen

El derecho a la propia imagen atribuye a su titular la potestad para disponer de su imagen física impidiendo su difusión salvo que medie su propio consentimiento. Las redes sociales permiten nuevas formas de reproducir la imagen de una persona y hacerla pública de forma instantánea, incluso sin que ésta se dé cuenta. Es obvio que, en la práctica, un usuario no suele preguntar a todas las personas que salen en una foto si tiene su consentimiento para publicarla. Puede que un usuario que quiera salvaguardar su imagen encuentre una foto suya circulando por las redes sociales sin permiso, e incluso verse etiquetado en la misma. Existe la opción de borrar la etiqueta, e incluso denunciar la foto, pero su imagen ya ha sido expuesta públicamente y podría haber copias en toda la red.

iv. Derecho a la libertad

El Título VI del Código Penal está orientado a proteger la libertad de los individuos, que se concreta en dos dimensiones: la libertad de obrar y la libertad de querer. Siempre que un particular prive a un individuo de cualquiera de estas dos libertades, estará incurriendo en un delito. Distinguimos en concreto cuatro posibles delitos contra la libertad: la detención ilegal, el secuestro, la amenaza y la coacción. A pesar de que las redes sociales podrían facilitar la comisión de delitos de detención ilegal o secuestro, dado que aportan información valiosa sobre el individuo (localización, hábitos...), nos centraremos en los delitos de amenaza y coacción.

Comete un delito de **amenazas** la persona que anuncia o advierte a otra, con el propósito de infundirle miedo, que le va a causar a él, a su familia o alguien vinculado con él, un **daño** que pueda ser constitutivo de los delitos de homicidio, lesiones, aborto,

torturas, contra la libertad, la integridad moral, la libertad sexual, la intimidad, el honor, el patrimonio... etc. intimidando al amenazado y privándole de su propia tranquilidad y seguridad.

En caso de amenaza se recomienda acudir directamente a la policía (autonómica, municipal o nacional), y presentar una denuncia. Según el caso, conviene solicitar que se tomen las **medidas cautelares urgentes** necesarias para avisar y proteger a las personas que corren peligro.

Es **coacción** la acción de impedir, con **violencia física o psicológica**, que una persona haga lo que la ley no le prohíbe hacer. También es **coacción** el obligar a una persona a hacer lo que no desea, ya se trate de hacer algo justo o injusto.

Debido al carácter inmediato de la publicación de contenido en las redes sociales, es fácil amenazar o coaccionar a otros usuarios, ya sea en público (muro) o en privado (mensaje, chat).

v. Libertad de expresión

Internet es una casa sin tabiques. Cada usuario es libre de publicar lo que quiera en las redes sociales, sometándose difícilmente al control de la plataforma que ofrece el servicio. Ciertas manifestaciones entrarían en colisión con otros derechos de los demás, establecidos en las legislaciones correspondientes (nacional, europea o internacional) o en los términos de uso de la red social que se utiliza.

Dada la imposibilidad de gestionar todo el contenido de una red social, éstas ofrecen herramientas para denunciar abusos. Quedará a criterio de los administradores de la red si el contenido infringe la Ley o las condiciones de uso. En tal caso eliminarían en primer lugar el contenido, y según la gravedad del abuso y el nivel de reincidencia, podrían cerrar el perfil o incluso emprender acciones legales contra el usuario.

Todos los derechos especificados en este apartado como “derechos vulnerables” podrían entrar en conflicto con la libertad de expresión, que debe por tanto verse limitada. Como ya hemos comentado, se debe proteger el derecho al honor, a la libertad, a la intimidad personal y familiar, así como a la propia imagen. Y como veremos a continuación, existe contenido protegido mediante propiedad intelectual e industrial.

vi. Propiedad intelectual

Las redes sociales están dando cada vez más importancia a la publicación de contenido gráfico, musical, audiovisual o de cualquier otro género sin que, generalmente, se pida autorización al titular de derechos. Es decir, suponen un vehículo para la reproducción, distribución, comunicación pública y transformación de obras protegidas mediante propiedad intelectual, justamente los derechos cuyo ejercicio exclusivo corresponde al autor, a no ser que se cedan expresamente por éste.

Las distintas plataformas son conscientes de la vulneración de estos derechos, y por tanto han habilitado un formulario de denuncia específico para este tipo de

infracciones. Cuando se publica contenido protegido por derechos de autor, no sólo se comunica públicamente, sino que éste es susceptible de ser copiado por parte de los usuarios, pudiéndose reproducirse a gran velocidad entre los internautas. Otro asunto delicado es el de la transformación. La Ley contempla que para hacer una parodia o cita no es necesario el permiso, pero en ocasiones resulta difícil y subjetivo discernir si un fragmento es una cita o plagio, o si la transformación de una obra supone una parodia. De todas formas, carece de sentido pragmático que la ley prohíba lo que no es controlable tecnológicamente.

En la era de la Sociedad de la Información (SI) resulta imposible controlar cómo accederán los ciudadanos a obras y prestaciones protegidas por los derechos de autor, por lo que se antoja necesario un cambio en la configuración de las leyes, de tal forma que se permita a los usuarios acceder a estas obras de la forma que deseen, al tiempo que se remunere correctamente a quienes ofrecen su tiempo, esfuerzo, talento y dinero a la creación de contenidos.

Asimismo, los usuarios han dejado de ser meros consumidores de obras para convertirse, gracias a las nuevas herramientas, en creadores, especialmente en redes sociales creativas como son Deviantart (creaciones gráficas), Flickr (fotografías) o MySpace (música). Por tanto será importante conocer qué ocurrirá con nuestras obras una vez que son subidas a una plataforma como MySpace o Tuenti, para evitar posibles abusos de los mismos. Hemos visto que en Tuenti o Facebook el propietario siempre será el usuario, y que su obra dejará de almacenarse en cuanto la elimine o se dé de baja de la red social. Al igual que MySpace, las cesiones se limitan al tiempo durante el cual el usuario utilice el servicio, sin capacidad de sub-explotación comercial, y por lo tanto, tendente únicamente a la correcta publicación de los contenidos aportados por los usuarios. No obstante en otras redes podría no ocurrir lo mismo.

vii. Propiedad industrial

La Propiedad industrial se vulnera en primer lugar por el uso sin consentimiento o autorización del titular de la marca del signo distintivo o logotipo. Aunque no exista interés de comercialización, el hecho de identificar una marca con una persona puede dañar la imagen de esa marca. Por ejemplo, si una persona usa el logo de una marca registrada como imagen identificativa, la marca estará en su derecho de indicar que hay violación de su derecho de marca. Asimismo, se vulnerarían los derechos de marca al desprestigiar una marca en concreto, si por ejemplo se afirmara en una red social “Consumir X provoca cáncer” sin justificación.

Por otro lado, se protegen las creaciones intelectuales, artísticas e industriales que aporten soluciones a problemas tecnológicos o de diseño o tengan una amplia proyección en el terreno económico. Por tanto, un usuario podría infringir la ley con publicar una imagen del pato Donald, por poner un ejemplo.

d. Sanciones

i. Delitos contra el honor

El delito de calumnia se castiga con multa de 4 a 10 meses. Si la calumnia se difunde con publicidad, es decir, por medio de la imprenta, radio, o similar (como sería el caso de las redes sociales), la pena será de **prisión** de 6 meses a 2 años, o **multa** de 6 a 24 meses. En estos casos, normalmente, también será **responsable** civilmente la persona física o jurídica propietaria del medio informativo por el que se difundiera la calumnia. Sin embargo las distintas plataformas se protegen alegando en sus términos de uso que “no se hacen responsable del contenido publicado por los usuarios”. Si el responsable del delito recibió o le prometieron alguna recompensa, además del castigo señalado, le será impuesta la pena de inhabilitación por un tiempo de 6 meses a 2 años.

Las injurias son castigadas con pena de multa de 3 a 6 meses y las hechas con publicidad, con multa de 6 a 14 meses. Si el responsable de la injuria recibe o le prometen recibir recompensa por la comisión del delito, podrá ser además inhabilitado para el ejercicio de su cargo público, oficio o profesión por un tiempo comprendido entre 6 meses y 2 años. En el caso de que las injurias se dirijan contra funcionarios públicos en el ejercicio de sus cargos, sobre faltas penales o infracciones administrativas, el acusado quedará libre de toda responsabilidad penal si acredita que sus manifestaciones son ciertas.

El responsable de un delito de injurias o calumnias puede quedar libre de responsabilidad penal si el ofendido o su representante legal, actuando en su nombre, le perdonan. Este “perdón” debe realizarse de forma expresa y ser anterior al inicio de la ejecución de la pena recogida en sentencia firme.

Si el acusado de un delito de injurias o calumnias reconoce ante la autoridad judicial que los hechos que atribuyó al perjudicado son falsos y se arrepiente de su actuación, el Juez o Tribunal le impondrá la pena inferior en grado, y podrá dejar de sancionarle con la de inhabilitación especial. El testimonio de la retractación del acusado se le entrega al ofendido por orden del Juez o Tribunal, y si éste lo solicita, podrá ordenarse que se publique dicho testimonio por el mismo medio que difundió la calumnia o la injuria.

Además de las consecuencias penales anteriormente descritas consistentes en multa, prisión e inhabilitación, el responsable de los delitos de injuria o calumnia está obligado a reparar el daño causado mediante una **compensación económica** a favor del ofendido, es la llamada ‘**responsabilidad civil**’.

En principio, será también responsable civil solidario junto con el ofensor, la persona física o jurídica propietaria del medio de comunicación a través del cual se haya propagado la calumnia o injuria. Dada la novedad de los medios, habrá que esperar para saber de qué forma se le atribuye también responsabilidad a las redes sociales.

ii. Delitos contra la libertad

El delito de **amenazas** está sancionado con prisión de 1 a 5 años, si la producción del daño en que consiste la amenaza se condiciona (por ejemplo, exigiendo una cantidad de dinero para evitar el perjuicio), o de 2 a 6 años de prisión si no se impone ninguna condición.

Las penas se graduarán en función de las circunstancias que rodeen a la comisión del delito y así se agravarán si se realizan por teléfono o cualquier otro medio de comunicación, o cuando se dirijan contra una multitud de personas.

Las amenazas con causar a otro un daño que no es constitutivo de delito también están penadas con prisión de 2 meses a 2 años o multa de 12 a 24 meses.

La pena aplicable al delito de **coacción** es la de prisión de 6 meses a 3 años, o multa de 6 a 24 meses, dependiendo de la gravedad de la coacción o de los medios que se empleen en la comisión del delito.

iii. Delitos contra la propiedad intelectual e industrial

Puesto que en las redes sociales no suele haber ánimo de lucro cuando se distribuye públicamente **contenido protegido por derechos de autor**, este comportamiento no es punible según la legislación española. El Código Penal describe las sanciones relativas a la propiedad intelectual e industrial en los artículos 270 a 276. El artículo 270 establece que se castigará con pena de prisión de seis meses a dos años y multa de 12 a 24 meses quien, **con ánimo de lucro** y en perjuicio de tercero, reproduzca, plagie, distribuya o comunique públicamente una obra sin la autorización de los titulares de los derechos de propiedad intelectual. El artículo 272 del Código Penal remite a los artículos relativos a las indemnizaciones en la Ley de Propiedad Intelectual (138 a 140).

El artículo 138 de la LPI establece que el titular de los derechos reconocidos en esta ley, sin perjuicio de otras acciones que le correspondan, podrá instar el cese de la actividad ilícita del infractor y exigir la indemnización de los daños materiales y morales causados. Además, la indemnización por daños y perjuicios debida al titular del derecho infringido comprenderá no sólo el valor de la pérdida que haya sufrido, sino también el de la ganancia que haya dejado de obtener a causa de la violación de su derecho. La cuantía indemnizatoria podrá incluir, en su caso, los gastos de investigación en los que se haya incurrido para obtener pruebas razonables de la comisión de la infracción objeto del procedimiento judicial.

En los artículos 273 y 274 del Código Penal se especifica que se castigará con la pena de prisión de seis meses a dos años y multa de 12 a 24 meses quien utilice, **con fines industriales o comerciales**, sin consentimiento del titular, con conocimiento de su registro, objetos amparados por derechos de Propiedad Industrial (artículo 273) o quien reproduzca un signo distintivo de un producto protegido (artículo 274). Como ya hemos comentado en el párrafo anterior, estas leyes no suelen ser de aplicación al no haber ánimo de lucro en las violaciones de estos derechos. Sin embargo sería de aplicación en el supuesto caso en que una marca buscara perjudicar a otra (para beneficiarse económicamente).

iv. Delitos relacionados con la protección de datos personales

La cuantía de las sanciones que impone la LOPD se gradúa en función de la gravedad de las infracciones (ver apartado 3.a.iii). Las infracciones leves, como supondría no atender a las solicitudes de rectificación o cancelación, se castigan con sanciones entre 601,01€ y 60.101,21€. Las infracciones graves, como por ejemplo Tratar datos especialmente protegidos sin la autorización del afectado, conllevan sanciones entre 60.101,21€ y 300.506,25€. Por último, las infracciones muy graves, como la recogida de datos de manera engañosa o fraudulenta, se persiguen con sanciones entre 300.506,25€ y 601.012,1€.

e. Delitos informáticos típicos de las redes sociales

i. Acceso a información confidencial

Las redes sociales, como Facebook, son el blanco favorito de piratas informáticos en lo que a robo de información personal se refiere. En julio de 2010, un experto en seguridad informática utilizó un código de programación para recolectar datos de 100 millones de perfiles de la red social Facebook²⁴. La lista llegó al sitio de descargas Pirate Bay y fue compartida por unos 1.000 internautas.

En un sentido estricto no supone un delito, dado que la lista ya estaba disponible en un directorio que recoge a todos los usuarios cuyo perfil está abierto aunque sea parcialmente²⁵. No obstante, que ahora esté organizada en una lista con nombres y números de identificación convierte en más sencillo para extraños recopilar direcciones de correo electrónico o datos sobre la ubicación geográfica de los usuarios de Facebook, entre otras informaciones. Además, las condiciones de uso de Facebook prohíben terminantemente el uso de programas para recopilar información de su red social, aunque ésta sea pública.

Lo que sí supone un delito es obtener información privada a través de la suplantación de identidad ya que se estará cometiendo un delito de usurpación de estado civil, y posiblemente de lesión de privacidad.

ii. Suplantación de identidad

Ya sea con el objetivo de obtener información confidencial o un beneficio económico, o simplemente el de causar daño, las redes sociales son el medio idóneo

²⁴http://www.elpais.com/articulo/Internet/Publicados/datos/millones/usuarios/Facebook/elpeputec/20100729elpepunet_1/Tes

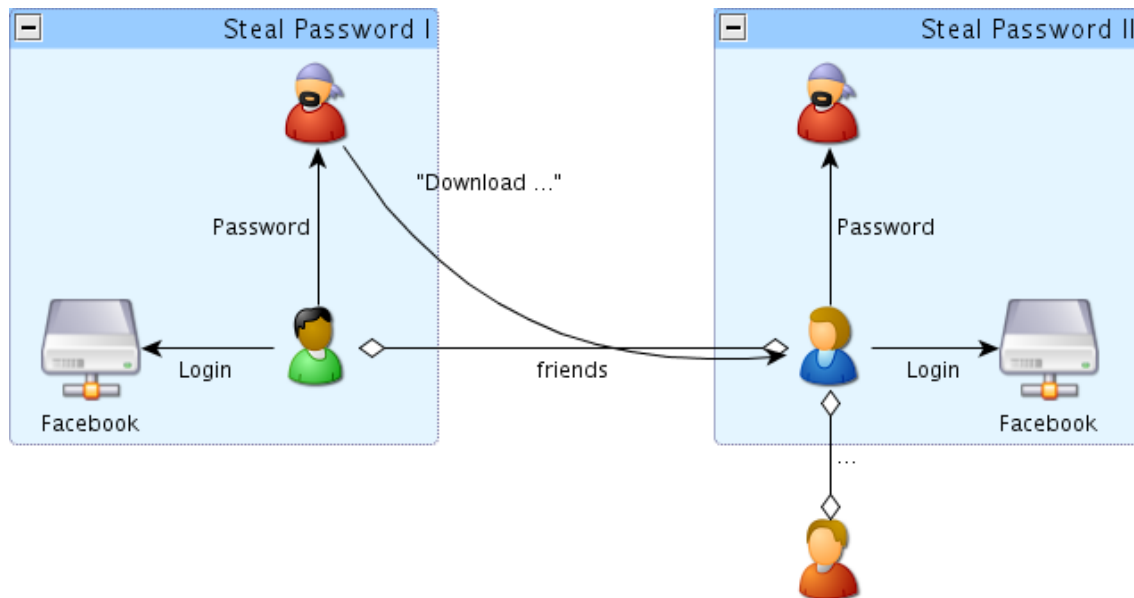
²⁵ <http://www.facebook.com/directory/>

para las prácticas de suplantación de identidad. Se puede acceder a mucha información confidencial, del perjudicado así como de sus amigos en la red social, con sólo un nombre y una contraseña.

Algunos buscan perjudicar a sus “enemigos”, como ha sucedido con los perfiles falsos de políticos (como Mariano Rajoy) o personajes públicos (José Mota). Los usuarios usurpadores podrían publicar información comprometida, dañando así gravemente la reputación de dichas personas. En un ámbito más doméstico, también se han dado casos de novios y novias despechados que perseguían el mismo fin con sus ex, o adolescentes que se hacen pasar por otros en las redes sociales para hacer una burla.

Por otra parte tenemos los hackers, que emplean técnicas más sofisticadas para obtener las contraseñas. Una de ellas es el phishing: el atacante implementa un sitio web idéntico a la página de inicio de la red social blanco del ataque y luego realiza envíos masivos no deseados (spam) de un vínculo a dicha página fraudulenta por correo o mensajes instantáneos, supuestamente a nombre de la misma red social. Asimismo, muchos usuarios no tienen claves lo suficientemente seguras. Los hackers tienen listas con las contraseñas más comunes, y también pueden utilizar la información de los perfiles para averiguar la contraseña (si fuera el nombre de un familiar o mascota, por ejemplo).

Tras acceder a la cuenta, el atacante puede entonces abusar de varias formas de esta información sonsacada. Podrá vender el registro de usuario, reunir más información del usuario atacado desde su perfil o enviar más mensajes spam a través de la plataforma de la red social desde la cuenta cautiva. Una vez que el atacante logra robar información de una cuenta, es muy probable que proceda a enviar vínculos que instalen un ladrón de contraseñas en los equipos de sus amigos, lo que resulta en una propagación exponencial, como vemos en la imagen.



Por tanto, si a algún conocido le roban su cuenta, todos sus contactos están expuestos. Y de este modo se abre la puerta a otros comportamientos delictivos como el chantaje o la estafa, los cuales veremos más adelante.

iii. Creación de perfiles falsos

Hay hackers que crean perfiles falsos con fines lucrativos e ilegales. Suelen conseguir muchos amigos, para generar confianza entre los nuevos usuarios que agrega al ver que ya es amigo de un amigo. Normalmente buscan agregar a gente del sexo opuesto (si se hacen pasar por una mujer agregan a hombres, y viceversa), y fingen tener una ocupación e intereses similares a sus víctimas, de las que se gana su confianza para llevar a cabo sus actividades delictivas (ver apartado siguiente).

Otros usuarios crean perfiles falsos con un fin aparentemente legítimo. Por ejemplo, el defensor del menor de la Comunidad de Madrid, Arturo Canalda, tiene un perfil falso de Tuenti para controlar a sus hijos, que afirma que este control es “algo necesario a pesar de que puede resultar controvertido porque alguien puede entender que es vulnerar la intimidad de los hijos”.

Por último, algunos internautas optan por incluir datos falsos en su perfil con el fin de conservar su privacidad. Es una práctica prohibida en las condiciones de uso, pero también extendida. Los usuarios escriben un pseudónimo o sus iniciales en lugar del nombre verdadero, fecha de cumpleaños falsa... Aunque esté contraindicado por la propia red, ya que de la misma manera se pueden crear perfiles falsos con fines oscuros, permitiría a los usuarios honrados que sólo les encuentren sus amigos a los que les hayan dado su pseudónimo de Facebook. Por otro lado, resultaría difícil encontrarlos si no se conoce dicho pseudónimo (para antiguos compañeros de clase, por ejemplo).

iv. Fraude informático

Muchos casos de suplantación de identidad y de creación de perfiles falsos en las redes sociales buscan cometer fraude. En cualquiera de los dos casos, una vez el usuario del perfil falso consigue la confianza del otro, le explica por ejemplo que está en un apuro y que necesita una pequeña cantidad de dinero. Algunos internautas caen en la trampa y transfieren el dinero a una cuenta, esperando que el otro usuario se lo devuelva.

v. Daño o sabotaje informático

La mayoría de los mensajes enviados mediante la técnica suplantación contienen un componente de ingeniería social que intenta engañar a la víctima (destinatario del mensaje) para que visite un determinado sitio web o para que descargue un programa en su equipo. En Twitter, uno de los peligros es el acortamiento de las URL. De esta forma, es más fácil enmascarar enlaces a páginas peligrosas.

4. Aplicaciones de las redes sociales

a. Las redes sociales y la empresa

El mundo laboral se adapta rápidamente a los nuevos fenómenos tecnológicos y sociales. Las redes se han convertido en una herramienta de comunicación más, al igual que el e-mail o el teléfono. También han revolucionado de manera notoria las estrategias de los departamentos de Recursos Humanos para captar o controlar a sus empleados. El triunfo mundial de las redes sociales ha propiciado la utilización de nuevos medios para cazar nuevos talentos o mantener controlados a los empleados. Las empresas tienen a su disposición nuevas formas para potenciar su marca y comunicarse con sus empleados o con clientes (reales o potenciales). Por otra parte, se ha criticado que los empleados utilicen dichas páginas para asuntos personales en el trabajo (como sucedía con el correo electrónico), así como se ha advertido del riesgo que entraña para la privacidad de las personas ser observado por el empleador.

Podemos dividir las redes sociales en dos grandes categorías: aquellas orientadas a nuestra vida personal (como Facebook o Tuenti) y aquellas orientadas a nuestra vida profesional (como LinkedIn o Xing). Aunque en principio el primer tipo de redes no se utiliza para buscar trabajo, brinda la posibilidad de hacerlo. Los usuarios pueden agruparse según grupos de interés (incluidos grupos profesionales), y las empresas las utilizan para recabar información valiosa.

i. Uso interno en las empresas

Dentro de las ventajas que suponen estas nuevas plataformas para el uso interno en las empresas, hablaremos en primer lugar del cambio en la **comunicación interna**. Debido a que se trata de herramientas relativamente nuevas, muchas compañías se hacen una idea errónea y sostienen que el uso de las redes sociales en el trabajo cuesta millones por la baja productividad. Por esta razón tratan de impedir a los empleados usar las redes sociales en el puesto de trabajo. Sin embargo, un estudio de la Universidad de Melbourne ha demostrado que los trabajadores que utilizan Internet para motivos personales en el trabajo son entorno a un 9 por ciento más productivos en el trabajo que los que no lo hacen.²⁶

En efecto, descansos cortos permiten una mayor concentración. Asimismo, este nuevo canal de comunicación motiva en mayor medida a los empleados. Contrariamente a otros canales tradicionales ofrece bidireccionalidad, permitiendo así realizar un trabajo más solidario. Es lo que se conoce como **empowerment**²⁷. Este consiste en el hecho de delegar poder y autoridad a los subordinados y de conferirles el sentimiento de que son dueños de su propio trabajo. Si guardamos la información de forma localizada en un lugar donde la gente puede fácilmente acceder a ella, entonces cada individuo tendrá un apoyo muy fuerte que le permitirá ser más creativo y eficiente.

²⁶ <http://www.telegraph.co.uk/technology/twitter/5093060/Twitter-and-Facebook-can-make-you-a-better-worker.html>

²⁷ http://www.elprisma.com/apuntes/administracion_de_empresas/definiciondeempowerment/

De este modo los empleados sentirán que pertenecen a una misma **comunidad**, lo que conducirá a un mejor ambiente de trabajo. Para la empresa, el hecho de tener a todos sus empleados en la misma red permite detectar cuál es el clima laboral que se respira en la organización y cuáles son los principales problemas en el día a día del negocio. Por el contrario, también podrá detectar algún si algún empleado habla mal de la compañía y tomar medidas al respecto.

Otra ventaja es la **gestión efectiva de los contactos profesionales**, a la que se saca un rendimiento muy importante, ya que puede servir para encontrar quien nos ayude a solucionar un problema, convertirse en cliente, proveedor, socio, etc. Las redes sirven también para comunicarse con los clientes y transmitirles lo que puede ser del interés de la empresa.

ii. Uso externo en las empresas

Las empresas disponen de una nueva herramienta para **captar nuevos empleados**. Los departamentos de Recursos Humanos y ‘headhunters’ (cazatalentos) están muy atentos a los perfiles de sus posibles fichajes. Un perfil permite saber mucho acerca de una persona: qué estilo de vida lleva, sus inclinaciones sexuales, sus aficiones e incluso su ideología o religión. Esta es una información muy útil a la hora de reclutar trabajadores, difícil de conseguir por otros métodos como la entrevista personal.

Es tal la influencia en las contrataciones, que las empresas casi no ponen anuncios. Según Elsa Izquierdo, consultora online de una compañía de cazatalentos, actualmente un 90% de las empresas localizan la gente online²⁸. Con ver sus perfiles personales y profesionales tienen suficiente como para saber si una persona les interesa. Contactan a la gente a través de redes como Xing o Facebook. Les resulta mucho más útil que poner un anuncio en Infojobs.

Lo importante es conseguir información distinta de la que proporcionan otros medios. A través de las redes sociales se puede realizar un **análisis de reputación** de los candidatos potenciales, de forma que sustituyen las referencias y cartas de presentación tradicionales. Asimismo permiten a las empresas establecer contacto con gente que nunca les enviaría su Currículum, porque ya tienen trabajo o por no saber de la existencia de dicha empresa.

• Marketing 2.0

Hoy en día, la presencia de las empresas en las redes sociales es necesaria para entrar en **contacto directo con el público**²⁹. Ya no hace falta un gasto exorbitado en campañas de marketing para que accedan a los consumidores y triunfen. Gracias a estas redes, el éxito vendrá más bien determinado por la creatividad y la habilidad de los expertos en implicar a los usuarios.

²⁸ http://www.soitu.es/soitu/2008/01/11/actualidad/1200056997_432019.html

²⁹ <http://www.suite101.net/content/la-comunicacion-empresarial-y-las-redes-sociales-a12039>

Somos testigos de un cambio fundamental: los clientes potenciales son ahora los mayores responsables del marketing. Es la empresa la que tiene que adaptarse a ellos, y no al revés. Lo cual vale la pena, ya que puede acarrear grandes ventajas. Las redes son un escaparate donde, por un lado, **una marca se muestra y se posiciona**, apoyando así a las campañas de comunicación tradicionales, y por otro, se capta valiosa información del público.

Al existir un diálogo, las empresas **se acercan a su público objetivo** y conocen mejor sus deseos y sus preocupaciones. La compañía podrá segmentar los clientes interesados de una manera más efectiva y conseguir datos que aportan voluntariamente (e-mail, información personal...). De este modo desarrollará campañas de imagen y de diferenciación estrechamente adaptadas. Formar parte de las redes sociales permite a una empresa controlar cómo perciben su marca los consumidores, especialmente si publican comentarios negativos. La mala publicidad que se propaga a velocidad de vértigo por una red social puede ser más dañina para la credibilidad de un producto que una crítica negativa en un periódico. En este caso sería capaz de reaccionar para mantener su imagen positiva.

- **El capital social**

Algunos expertos³⁰ afirman que en la actualidad, el capital financiero es la suma del capital social más el capital cultural. Explicar estos conceptos a continuación.

El **capital social** representa el conjunto de personas dispuestas a apoyar ideas, a escuchar lo que uno tiene que decir, y que tienen interés en mantener el contacto. Si el capital financiero se puede asimilar al “dinero”, el capital social se asemeja al concepto de “amigos”, aunque en realidad se refiere a algo más que los individuos físicos dispuestos a comprometerse con el trabajo de alguien.

En la mayoría de los casos, el capital social se genera offline y se representan de manera online a través de las plataformas de redes sociales, que permiten mantenerlo de forma explícita para un uso y referencias futuros. Tras contactar cara a cara con una persona, resulta mucho más fácil mantener la relación a través de dichas plataformas. En el ámbito empresarial, por lo general se crean **lazos débiles**, que podrían prosperar en un futuro. Pero para ello habrá que mantener la relación y avivar el interés del contacto. Para ello, ya no serán necesarias llamadas de teléfono ocasionales o enviar e-mails de cuando en cuando para asegurar que la otra persona conserva los datos de contacto. Las listas de contactos garantizan el acceso a los demás cuando sea de interés, así como a sus recursos, dado que el capital social se refiere tanto a la red de contactos como al acceso a los recursos que éstos pueden proporcionar.

No obstante, el capital social por sí solo no es suficiente como para generar capital financiero. Hace falta un **capital cultural**, asimilable a una “influencia”. Este engloba los conocimientos, la experiencia y las conexiones de una persona, esto es, la cantidad de influencia y ventajas que una persona aporta a la sociedad. La gente con un

³⁰ 33 Million People in the Room. Juliette Powell. FT Press 2008.

gran capital social ejerce influencia sobre sus amigos. Aquellos con capital cultural tienen influencia sobre la industria y el mundo a una escala mayor. Este capital aporta credibilidad, creando así mayores oportunidades y perspectivas para la organización.

A la hora de crear una marca online, se debe obrar paso a paso. Hace falta tiempo para afianzar la reputación asociada al capital cultural, sin importar lo respetada que sea una marca offline. Resulta por tanto conveniente crear primero el capital social, y después añadirle valor y generar confianza en la red. De este modo aumentarán las oportunidades dentro de la red, conduciendo así la suma del capital social y cultural a la generación de un capital financiero.

b. Las redes sociales y la política

En los últimos años, la práctica política ha tenido que adaptarse y hacer uso de los nuevos medios digitales para conseguir sus objetivos. Esto supone enormes cambios para los partidos en cuanto a la forma de llegar a sus electores. Las distintas organizaciones políticas ya no sólo se dirigen a aquellos normalmente involucrados en la actividad política, sino a todos aquellos que no muestran interés por ella. Es lo que se llama la democracia electrónica, que aporta usabilidad y flexibilidad para todos los usuarios.

Por otra parte, las personas se ven dotadas de un **nuevo poder**. Ahora todo el mundo es capaz de transmitir un mensaje a muchos, es decir, cada persona se puede convertir en nodo difusor. De las redes sociales pueden surgir muchas iniciativas e ideas, siendo así el canal idóneo para promover acciones por parte de los usuarios. Además, contrariamente a otros medios, éstos encuentran una **retroalimentación** dentro del mismo canal. Los medios tradicionales (televisión, radio, prensa escrita) siempre se han caracterizado por la unidireccionalidad. Ahora, cualquier puede exponer su opinión, y quien lo desee expresar su conformidad o rechazo de forma instantánea. Otra gran ventaja de estos nuevos medios es que por lo general se conoce al emisor de un mensaje. Mientras el presentador del telediario o el autor de un artículo de periódico nos son desconocidos y confiamos en ellos relativamente, se supone que los contactos que uno posee en su red social son gente conocida, lo que otorga credibilidad a su mensaje por parte de los lectores.

En este apartado explicaremos y expondremos ejemplos sobre los usos de las redes sociales en la política según la clasificación realizada por Antoni Gutiérrez-Rubí, experto en comunicación política. Estos incluyen tanto los usos por parte de los dirigentes como de los usuarios en general: resistencia, censura, agresión, denuncia, guerra, comunicación, organización, difusión de noticias y actos políticos y participación.

1. Resistencia

Se define la resistencia política como las prácticas y movimientos sociales subversivos o clandestinos de lucha contra un sistema, o más específicamente, contra un poder político o militar en una región. Las redes sociales ofrecen el medio idóneo para que los opositores de un régimen se comuniquen de forma relativamente anónima y en tiempo real. Se pueden emplear para denunciar situaciones inaceptables para los usuarios (burlando de este modo a la censura), para consolidar un grupo de resistencia y actuar de forma conjunta (organizando manifestaciones, por ejemplo) o incluso crecer como grupo convenciendo a nuevos usuarios que tienen acceso a estos medios.

Estudiaremos el caso concreto de Venezuela, donde los opositores al régimen de Chávez emplean la plataforma Twitter para denunciar la falta de libertades. Tras cierres de emisoras y encarcelamiento de reporteros contrarios a las ideas del partido, la oposición ha encontrado en Internet el único vehículo válido para expresar su opinión sin censuras. Según la agencia Reuters, Twitter cuenta con más de 200.000 cuentas

abiertas en Venezuela, lo que sitúa al país a la cabeza del ranking en Latino América por índice de penetración de la red de microblogging. Por ejemplo, desde la etiqueta #FreeVenezuela se han difundido 33.782 mensajes con una consigna: «Venezuela, zona de desastre para la libertad de expresión»³¹.

Debido a la dificultad de control por parte de las autoridades venezolanas, el presidente Hugo Chávez llegó a afirmar que “Twitter es un instrumento de terrorismo”. No obstante, en el mes de abril de 2010 abrió una cuenta en la misma red social³², como parte del contraataque mediático frente a las presuntas campañas en contra de su Gobierno "revolucionario". También ha abierto una cuenta Diosdado Cabello, vicepresidente del Partido Socialista Unido de Venezuela (PSUV), que ha hecho un llamamiento a los 7 millones de militantes de su partido para emprender una verdadera guerra dentro de Twitter contra los opositores del régimen.

2. Censura

Algunos gobiernos han trasladado la censura que ejercían en los medios tradicionales a las nuevas tecnologías. La diferencia fundamental es que las fronteras nacionales son mucho más permeables en Internet. Aunque un país corte el acceso a alguna de sus páginas web, los residentes de ese país seguirán teniendo acceso a otras procedentes de otros países. Un gobierno puede tratar de evitar el acceso a sus ciudadanos a ciertas páginas, a pesar de no tener control sobre ellas, mediante procedimientos de lista negra por ejemplo.

La censura de Internet es un procedimiento muy complejo y costoso. Los organismos reguladores utilizan procedimientos técnicos como el bloqueo de IP o el filtrado de DNS y URLs. Por otra parte, los usuarios cuentan con métodos para evitar estos procedimientos de censura: páginas web alojadas en servidores proxy, redes privadas virtuales o software diseñado a tal efecto.

El objetivo es controlar todas las comunicaciones del país. Esto incluye en primer lugar las comunicaciones internas (para interceptar cualquier contenido que sea considerado subversivo), las comunicaciones procedentes del exterior (para manipular la opinión pública a través de las agencias de noticias oficiales), y las dirigidas al exterior (del mismo modo, el Estado ofrecerá sus noticias oficiales, cuidando la imagen de cara al exterior).

El caso más flagrante en la actualidad es el de China. A pesar de ser el país con más internautas del mundo (300 millones), sufre también una de las censuras de contenidos más duras de la Red, especialmente en momentos de tensiones políticas o fechas 'sensibles' para el gobierno comunista. Ya en 2008, China bloquea YouTube y 'The Guardian' tras los disturbios en el Tíbet³³, para evitar que se colgaran vídeos sobre las protestas de Lhasa. En junio de 2009, bloquea Twitter y Hotmail en vísperas del

³¹ <http://www.abc.es/20100216/medios-redes-web/twitter-chavez-201002162010.html>

³² <http://www.abc.es/20100427/medios-redes-web/chavez-tiene-cuenta-twitter-201004271922.html>

³³ <http://www.elmundo.es/navegante/2008/03/17/tecnologia/1205745625.html>

aniversario de Tiananmen³⁴ y finalmente corta el acceso a Facebook en julio debido a los violentos enfrentamientos en Urumqi³⁵.

3. Agresión

Desde la aparición de Internet, ha sustituido progresivamente a los medios de comunicación tradicionales (como revistas clandestinas) para convertirse en el principal vehículo de comunicación de los movimientos de ultraderecha. Las ventajas que encuentran son similares a las que protegen a los grupos de resistencia: principalmente anonimato y eficacia como herramienta de propaganda. Sin embargo, aquí no hablamos de personas que persiguen unas libertades dentro de un país cuyo gobierno se las niega, sino de grupos anti-democráticos que fomentan el odio y promueven la violencia racial, el antisemitismo, la homofobia y el terrorismo.

Según un informe de Centro Simon Wiesenthal³⁶ de mayo de 2009, basado en más de 10.000 páginas web, portales, blogs, chats, videos y juegos, se ha registrado un incremento del 25% en el número de grupos 'problemáticos' en las redes sociales en Internet durante el año anterior al estudio. En redes sociales como Facebook no resulta difícil encontrar grupos que incitan al odio hacia otras razas o ciertos colectivos. Por ello los responsables de Facebook aseguran hacer un esfuerzo para eliminar todas las páginas o grupos que violen sus condiciones de uso. Pero con más de 500 millones de usuarios activos, hasta que se borran, los grupos han proliferado en la red. Algunas páginas cobran tal importancia que derivan en redes sociales independientes, como New Saxon, “una red social para gente de ascendencia europea”, gestionada por un grupo neo-nazi estadounidense llamado Movimiento Nacional Socialista.

Otro hecho destacable es la eliminación de varios grupos neonazis de la plataforma Facebook.³⁷ Eran usados por neonazis italianos para instar a la violencia contra el colectivo gitano en Italia. Facebook ha asegurado que no revisa los perfiles antes de que sean publicadas, pero sí tiene un equipo dedicado a controlar el cumplimiento de las condiciones de uso, y que por tanto prohíben la publicación de cualquier artículo agresivo, u objetable por delitos raciales, étnicos o de otro tipo.

En una sociedad democrática hacer frente a estas trincheras del odio es clave. El Movimiento contra la Tolerancia propone una serie de medidas como, por ejemplo, el reconocimiento de la especificidad del delito de odio y la generación de unas estadísticas oficiales por parte del Ministerio del Interior, algo que realizan todos los países europeos a excepción de cinco.

³⁴ <http://www.elmundo.es/elmundo/2009/06/02/internacional/1243963540.html>

³⁵ <http://www.elmundo.es/elmundo/2009/07/08/navegante/1247035807.html>

³⁶ <http://www.wiesenthal.com/site/apps/nlnet/content2.aspx?c=IsKWLBpJLnF&b=4441467&ct=6994349>

³⁷

http://www.elpais.com/articulo/Internet/Facebook/expulsa/comunidad/varios/grupos/neonazis/20elpepuint/20081117elpepunit_1/Tes

4. Denuncia

Gracias a su gran poder de convocatoria entre los ciudadanos, las redes sociales permiten transmitir rápidamente un mensaje a gran cantidad de personas. En ocasiones estos mensajes no aportan información nueva y buscan actuar frente a los poderes políticos. Y en otras se persigue informar a la gente de una situación contra la cual se considera que habría que actuar. La denuncia se encontraría a caballo de estas dos posturas: el fin es de informar y actuar para luchar contra una situación determinada.

A modo de ejemplo, en diciembre de 2009, más de mil personas se manifestaron contra la corrupción en Palma de Mallorca³⁸. Dicha manifestación había sido convocada por un grupo creado en la red social Facebook, que ha superado las 3.000 adhesiones, "puramente ciudadana al margen de todos los partidos políticos". Meses después, Facebook volvió a erigirse como máximo exponente contra la corrupción en Baleares, ya que el mismo grupo convocó una nueva protesta coincidiendo con la declaración judicial de Jaume Matas. La peculiaridad de estas acciones es que no están convocadas por ninguna organización como se hacía tradicionalmente, sino por un grupo de una red social formado por gente que en su mayoría no se conoce, pero persigue una finalidad común.

5. Guerra

Otra práctica política efectuada a través de las redes sociales es el uso como arma de guerra. Es evidente que no nos referimos a una guerra de trincheras, sino a la guerra mediática, que sirve de apoyo para otro tipo de acciones bélicas. Un ejemplo claro sería la propaganda israelí. En los últimos ataques perpetrados en los territorios palestinos, además de los bombardeos, el gobierno israelí también ha "bombardeado" al mundo con propaganda. Es lo que se denomina "guerra blanda".

Esta campaña intensiva de relaciones públicas tiene como objetivo mejorar la reputación de Israel en el extranjero, mermando así la condena internacional a los ataques indiscriminados contra la población civil de Gaza. El gobierno israelí contrató a expertos en Internet que diseñaron una guerra informativa. Esta guerra incluye un plan para transmitir imágenes positivas del estado judío por toda la Red, así como la adopción de perfiles especiales de Israel en redes sociales, en las que interactúan cambiando el estado cada vez que cae un cohete Qassam sobre Israel, por ejemplo. Asimismo, durante el asalto a la Flotilla de la Libertad de Gaza (mayo de 2010), el Ministerio de Asuntos Exteriores israelí puso de nuevo en marcha su maquinaria de publicidad de comunicación, enviando a cientos de twitteros de todo el mundo un mensaje en el que pretendían disfrazar a los activistas de pseudo-terroristas³⁹.

³⁸ <http://www.elmundo.es/elmundo/2009/12/12/baleares/1260622017.html>

³⁹ <http://guerreando.wordpress.com/2010/06/07/israel-me-ha-mandado-un-tweet-el-poder-de-las-redes-sociales/>

6. Comunicación

Las redes sociales resultan atractivas para los políticos como herramienta de comunicación. Algunos partidos han surgido y se han dado a conocer gracias a estas plataformas, otros ya existentes las han utilizado para hacer campaña y recabar información de los ciudadanos, además de informar, involucrar y establecer vínculos con su electorado. A pesar de ello, Internet es un arma de doble filo. Las redes abiertas escapan al control de los creadores y las críticas y protestas surgidas de la creación de una página de un partido podrían no compensar el esfuerzo. Asimismo, una página o grupo en una red deben mantenerse activos, o de lo contrario se volvería en contra de la persona involucrada ya que transmitiría una imagen negativa.

La creación de nuevos partidos políticos ha acompañado el crecimiento de la popularidad de las redes sociales. Un ejemplo es el Partido de Internet, plataforma legal nacida en España en 2008 creada por Héctor Pérez, ingeniero de telecomunicaciones. Este partido promueve que todos los ciudadanos participen activamente en las decisiones que se toman en el congreso. A pocas horas de dar a conocer su proyecto, centenares de personas comenzaron a unirse a él para colaborar en una idea que a muchos se les había pasado por la cabeza, pero pocos se atrevían a definir. Desde enero de 2010, el Partido de Internet está oficialmente registrado en la lista de partidos con las siglas "INTERNET" y cuenta con más de 1000 partidarios.

Los nuevos medios sociales ofrecen ventajas claras para los políticos. Su característica más llamativa es que permite un fácil acceso al personaje político por parte de los ciudadanos, algo impensable hasta el momento, así como una actuación rápida llevada a cabo por los partidarios. Existen dos estrategias: top-down, que se refiere a los simpatizantes pasivos, implica que el ciudadano ayuda a los fines del partido sin involucrarse activamente, haciéndose fan de una página relacionada con la política, por ejemplo. Por el contrario, la estrategia bottom-up, la cual se promueve de manera mucho más eficaz en las redes sociales, permite a los simpatizantes proponer ideas e interactuar. La página personal de un político nos da una impresión de acercamiento, e incita a escribir, preguntar y dialogar con éste, esto es, a involucrarse más con el partido en cuestión.

Al igual que las páginas web y blogs, un perfil en una red como Facebook permite informar de forma clara. Se pueden publicar propuestas en el muro, o enviar mensajes masivamente a los amigos y fans. Esta segunda opción da pie a lo que se denomina *micropolítica*: se puede personalizar los mensajes hasta casi individualizarlos. Es una manera económica de hacer el tradicional *puerta a puerta*. La lista de seguidores puede ser una mina de oro de información, que permite hacer un buen seguimiento de quién votará a quién, y catalogar a los posibles votantes para mandarles información adecuada, e incluso incitar a quién participa más activamente a hacer un donativo.

7. Organización

Para mantener un mayor control e imponer estrategias políticas determinadas, algunos partidos políticos han desarrollado sus propias redes sociales cerradas para sus

simpatizantes y afiliados, como es el caso de Obama, quien ha hecho uso de un sofisticado paquete de herramientas online para ganar las elecciones de 2008.⁴⁰

La plataforma tecnológica, exclusivamente diseñada por la compañía Blue State Digital para el activismo online, permitió crear, gestionar y publicar campañas de apoyo, gracias a las cuales se recaudaron millones de dólares para la campaña. El equipo Obama tuvo la habilidad de integrar a la perfección la actividad online con las actividades en el mundo real. Ha sabido poner estas tecnologías en el corazón de su campaña, aprovechando así el entusiasmo colectivo por cambiar el mundo para obtener gran cantidad de información acerca de los simpatizantes, crear eventos, seducir a votantes indecisos, y lo más importante: convertir el hecho de donar dinero en un evento social.

8. Difusión de noticias

Dentro de las redes sociales, se genera constantemente contenido sin intermediarios. Un gran número de usuarios de estas redes actualizan su perfil y suben contenidos a Internet a través de su teléfono móvil. En cualquier parte del mundo puede haber un “informador” espontáneo en caso de ocurrir un acontecimiento relevante. Tradicionalmente, había que esperar que los medios estuvieran al tanto y transmitieran la noticia por televisión, radio... Proceso en el cual se podía producir un filtrado o incluso censura por parte de los gobiernos. Al subirse la información directamente a la red, el mundo se entera en tiempo real de atentados, accidentes, guerras, sin que los poderes políticos puedan intervenir en la difusión de dicha información.

9. Actos políticos y participación

Por último, analizaremos la potencia participativa de las redes sociales. Ya hemos visto que permiten juntar a un gran número de personas con un interés común. Veamos el caso de la plataforma “Salvem el Cabanyal”. Este colectivo de Facebook, que reúne a más de 23.000 personas (a fecha de septiembre de 2010), aboga por la conservación del barrio del Cabanyal en Valencia, a través de un plan de rehabilitación de todos los poblados marítimos. Aunque el mero hecho de formar un grupo multitudinario no hará cambiar las cosas, sí se pueden organizar actos de protesta y conseguir frenar el avance de programas políticos contrarios a la voluntad de un número importante de ciudadanos.

En conclusión a este apartado, vemos que las redes sociales han dotado a la política de una nueva dimensión mucho más dinámica y difícil de controlar. Algunos ciudadanos las utilizan para reivindicar lo que consideran justo y evitar así censuras por parte de gobiernos opresores, otros las utilizan para juntarse con otros ciudadanos y participar activamente en la vida política, incluso creando sus propios partidos y organizaciones políticas, legítimas o no. Los gobiernos también echan mano de estas

⁴⁰ http://www.tendencias21.net/Las-redes-sociales,-fundamentales-para-el-triunfo-de-Obama_a2717.html

plataformas: algunos las quieren bloquear para controlar a la población (China, Irán...), otros las usan para hacer propaganda (Israel), del mismo modo que algunos partidos han conseguido triunfar gracias a las campañas que han llevado a cabo en ellas (como en el caso de Obama en las elecciones de 2008).

c. Uso en la docencia

Tradicionalmente, no se podía concebir la enseñanza sin un importante componente presencial. La enseñanza a distancia existía antes del desarrollo de los medios tecnológicos actuales, pero sin duda ha sido gracias a éstos que está teniendo un papel mucho más importante en nuestra sociedad. Ya en los años 90, con la expansión de Internet, los diferentes organismos educacionales comenzaron a ofrecer contenidos a través de la red, y se empezó a utilizar el correo electrónico como medio de comunicación entre alumnos y profesores.

No obstante, la capacidad de interactuar con los contenidos era prácticamente nula, hasta que surgió la Web 2.0. En la actualidad, tanto estudiantes como docentes se han convertido en lectores a la vez que escritores de contenido, ya que ahora tienen acceso a espacios en los que cualquier usuario, sin necesidad de conocimientos tecnológicos, puede aportar experiencias y compartir lo que quiera.

i. Motivación

Anteriormente, la educación a distancia se consideraba pasiva y puramente autodidáctica. Hoy en día, a través de los nuevos canales electrónicos, un curso online bien elaborado puede ser más interactivo que uno presencial. La Red ha pasado a ocupar un lugar más activo, se han desarrollado nuevas herramientas que permite el intercambio de información entre alumnos y docentes, de forma síncrona o asíncrona, sin limitaciones espacio-temporales.⁴¹

Sin embargo, siempre habrá algunas cosas que no se puedan sustituir por ordenadores. En centros con programas virtuales como la escuela IE realizan dos o tres reuniones presenciales, ya que opinan que si la gente se conoce, aunque solo sea una vez, después la comunicación por foros de Internet es más fluida. Además, aunque los métodos por Internet se consideran perfectos para enseñar procedimientos, todavía es necesario dar clases presenciales para la enseñanza de aptitudes. No es lo mismo impartir un curso sobre la literatura española durante el Siglo de Oro que enseñar a un comercial a vender. Aquí es donde lo que se denomina B-learning (blended learning) cobra sentido. Consiste una formación semi-presencial, que incluye clases y actividades presenciales y e-learning. De este modo se aprovechan las ventajas tanto de la enseñanza a distancia como de la presencial.⁴²

Por otra parte, la Sociedad de la Información exige un cambio en el modelo didáctico. Se aboga por el abandono de las prácticas de memorización pura y dura en favor de metodologías socio-constructivistas, esto es, centradas en los estudiantes y en el aprendizaje autónomo y colaborativo. Las redes sociales así como otros entornos de la Web 2.0 constituyen un instrumento idóneo de metodologías socio-constructivistas al situar el estudiante en el centro del proceso de aprendizaje.

⁴¹ Juan José de Haro. Revista DIM: Didáctica, Innovación y Multimedia, Nº. 13, 2009

⁴² <http://jjdeharo.blogspot.com/2008/11/la-redes-sociales-en-educacin.html>

Según una encuesta reciente realizada en la Universidad de Granada de cara al uso de las redes sociales en un contexto didáctico, el 89% de los estudiantes utilizan alguna red social, en su mayoría varias veces al día y a través de sesiones superiores a diez minutos. Ateniéndonos al éxito de estas redes, ¿para qué buscar herramientas informáticas nuevas si existen otras que funcionan y tanto alumnos y profesores ya saben utilizar?

ii. Ventajas

La principal ventaja que proporcionan las redes sociales en la docencia es su indudable utilidad como **medio para fomentar el contacto**, el diálogo y la comunicación entre alumnos y profesores. Un aula es en sí una pequeña sociedad formada por el profesor y sus alumnos, siendo por tanto un lugar idóneo para la colaboración y el trabajo conjunto. Estas redes gozan de una excelente capacidad para mantener en contacto un gran número de personas. La comunicación directa entre profesor y alumno se convierte en algo muy sencillo, bien de forma pública a través de su “muro”, mediante mensajes privados de correo electrónico interno o mediante mensajes enviados a todos los miembros del grupo. Esto propicia un sentimiento de cercanía y de pertenencia a una comunidad educativa.

El uso de redes sociales para el estudio es un **elemento de motivación** para el estudiante. En la red puede reflexionar, argumentar, discutir y tomar posiciones. Es lo que se denomina aprendizaje informal, en oposición al formal. Estas plataformas también permiten el desarrollo de destrezas clave en nuestra sociedad, como la creatividad, la independencia y la espontaneidad.⁴³ Los estudiantes tienen la oportunidad de exteriorizar sus pensamientos y personalizar sus propias páginas. Por otra parte dejan de depender tanto del maestro, volviéndose responsables de su propio aprendizaje y construyendo su conocimiento por sí mismos. Los alumnos se convierten en los principales actores, siendo los docentes actores de reparto, lo cual mejora notablemente el ambiente de trabajo.

Cuando un profesor se apoya junto a otros en las tecnologías de Internet y tienen un elevado número de alumnos, la dispersión en las fuentes de información puede dificultar la eficacia de la tarea educativa. Las redes sociales permiten **centralizar en un único sitio** todas las actividades docentes. Algunas como Ning o Elgg, las cuales trataremos en el siguiente apartado, permiten una gestión muy eficiente cuando hay implicado un gran número de alumnos y profesores. Es más, cuanto mayor sea el número de miembros de una red social, mayor será su productividad. Se considera eficaz una red a partir de 100 alumnos, y que por tanto una red social de 500 miembros será mucho más efectiva que una de 100. Parece que existe un fenómeno de retroalimentación de forma que un incremento en el número de usuarios en la red produce un aumento todavía mayor de la actividad de la misma.

La creación de **grupos** según las necesidades de cada momento otorga al profesor un mayor control y una mejor coordinación con sus alumnos. Los grupos son

⁴³ Francisco José Ruiz Rey. Revista DIM: Didáctica, Innovación y Multimedia, Nº. 13, 2009

de una gran plasticidad y pueden usarse, en otras muchas cosas, para los fines que veremos a continuación (De Haro, 2008). Para una asignatura concreta, donde el profesor ponga las tareas, cuelgue enlaces a recursos externos, avisos a los alumnos y se debatan temas de clase. En grupos de tutoría, el tutor puede establecer diálogos sobre temas que considere oportunos. Por último, se pueden hacer grupos de poco alumnos para que estén en contacto a la hora de hacer los trabajos de las asignaturas.

Otra gran ventaja es el **carácter generalista** de las redes sociales. La necesidad de formación es mínima, ya que todos utilizan el mismo recurso, y la red social funcionará exactamente igual independientemente de la asignatura, profesor o grupo que estemos usando. Además, ofrecen muchas herramientas generales y visibles por todos los miembros de la red como un calendario de eventos, blogs, foros de discusión, zonas para contenido audiovisual...

Las **redes cerradas** suponen una mejor opción, ya que son perfectamente **controlables** por los administradores de las mismas, que pueden eliminar contenido inapropiado o bloquear a usuarios que den problemas. Además, en el caso de los menores, sirven para evitar la difusión de sus nombres y otros datos que permitan su identificación, como puede ser la fotografía de su perfil. Los alumnos tendrán que aprender sobre el comportamiento social básico, o sea, conocer dónde están sus límites y respetar al centro educativo.

Nos hemos centrado en los alumnos, pero las redes sociales pueden ser de gran utilidad para la comunicación entre **profesores** de un mismo departamento o una misma asignatura, o a un nivel superior, para coordinarse con la dirección del centro educativo mediante comunicaciones internas. También pueden fomentar la colaboración los profesores y los lazos de unión entre ellos. En el marco de la educación pre-universitaria, hacer una red social para padres puede ser beneficioso para el rendimiento de los escolares ya que aumentaría la implicación de éstos en la educación de sus hijos.

Por último, la ventaja más clara de todas, que es el **uso práctico de las TIC**, tanto en el aula como fuera de ella. Se habitúa desde el principio a los alumnos a unas infraestructuras telemáticas, generalmente basadas en los servicios de Internet. Gracias al uso de estas herramientas, se desarrollan y mejoran las competencias digitales de los estudiantes, desde la búsqueda y selección de información y su proceso para convertirla en conocimiento, hasta su publicación y transmisión por diversos soportes.

iii. Plataformas

Existen plataformas específicas para la educación desde la era del Web 1.0, siendo Moodle una de las más populares. Sirven de apoyo a la enseñanza presencial, ya que incluyen herramientas de administración de usuarios, cursos, cuestionarios, evaluaciones... Es decir, todo lo que puede hacer falta a un profesor para realizar sus actividades docentes. Sin embargo, en éstas la participación y colaboración brillan por su ausencia, aunque dispongan de wikis (o diarios) y foros, estos sólo se utilizan para resolver dudas importantes.

Contrariamente a las redes sociales que ya conocemos, donde se puede compartir gran variedad de archivos, en estos sistemas éstos son generalmente subidos por el profesor, salvo las prácticas o trabajos de clase que pueden subir los alumnos y compartirlo únicamente con el profesor. Por tanto estos sistemas son mucho más verticales y no tienen tanta flexibilidad.

Las principales redes sociales utilizadas con fines docentes son Ning y Elgg. Ning es una plataforma online para usuarios que permite crear sitios web sociales y redes sociales, sea cuál sea el ámbito de aplicación. Su principal característica es que permite que cualquiera cree su propia red social personalizada para un tema en particular o necesidad, dirigida a audiencias específicas. No requiere instalación de software, y las redes creadas en este sistema son independientes las unas de las otras, por lo que no se producen las interferencias existentes en otras redes sociales más generales. Cabe destacar que en el caso de redes para alumnos menores de edad, se ha eliminado la publicidad. La gran desventaja de esta red social es que es de pago. Afortunadamente existen alternativas gratuitas interesantes, como Elgg.

Elgg es otra plataforma similar de código abierto que ofrece herramientas de blog, trabajo en red, comunidad, recolección de noticias vía feeds e intercambio de archivos. Todo puede ser compartido con los usuarios. El problema de Elgg (en su versión gratuita) es que requiere la instalación de software en los servidores propios, lo que supone un gasto para el centro y puede acarrear problemas. Este sistema ofrece también un servicio de alojamiento en el que pasa a ser más similar a Ning, si bien este es pago.

En el ámbito universitario, los alumnos son mayores de edad y por tanto existe una menor preocupación por la privacidad. Algunas universidades, como la Universitat Oberta de Catalunya (UOC), han optado por emplear Facebook, una plataforma abierta, para crear un entorno virtual de aprendizaje, basado en el uso de recursos y metodologías centrados en la participación y colaboración de alumnos y profesores. La ventaja es que en la mayoría de los casos los usuarios no necesitan cambiar de plataforma. Sin embargo los profesores pierden poder como administradores, y se pierde el control sobre la privacidad de los contenidos.

Asimismo, algunos profesores se han planteado emplear Twitter como herramienta docente. Además de las virtudes ya comentadas de cualquier red social de cara a la enseñanza, como la inclusión de contenido o enlaces externos, la gran ventaja es la limitación de 140 caracteres, que proporciona un gran dinamismo a la interacción entre alumnos y profesores, de modo que se estimula la participación. Dado su carácter informal, permite intercalar cuestiones docentes con comentarios más banales, con lo que la sesión gana en agilidad y pierde en solemnidad.

De cualquier manera, los profesores demandan algunas funcionalidades que las plataformas para crear redes sociales (Elgg o Ning, entre otras) o las redes sociales generales (Facebook, Twitter...) no poseen. Por tanto a día de hoy puede resultar conveniente la combinación de un entorno virtual “tradicional” y de una red social creada específicamente con fines educativos, como sería la combinación Elgg + Moodle, o cualquier red más la plataforma utilizada en la universidad. Otra posibilidad es la evolución de los entornos educativos ya existentes de modo que incluyan las funcionalidades de las redes sociales.

Hemos visto por tanto que algunos profesores están dispuestos a emplear las redes sociales como herramienta de apoyo en su actividad docente. En un contexto de paradigma cambiante en la enseñanza, donde se valora cada vez más la participación e interacción por parte del alumno, estas redes otorgan grandes ventajas. Pero siguen quedándose cortas respecto a las funcionalidades que se esperan, y que sí se incluían en otras plataformas anteriores. Al tratarse de un fenómeno muy nuevo, es de esperar que en cuestión de años empiecen a surgir redes específicas perfectamente adaptadas a tal fin.

Hemos observado que el espacio de las redes sociales se somete difícilmente a una legalidad que todavía debe adaptarse a las nuevas plataformas de comunicación, para regular su uso lo mejor posible. Este hecho, sumado a la imposibilidad técnica de controlar todo lo que circula por las redes sociales, permite que ciertos comportamientos, considerados delictivos en otros entornos, queden impunes. A esto hay que añadirle la escasa percepción de peligro por parte de los usuarios, que al fin y al cabo son los máximos responsables de su propia intimidad. De nada sirve publicar nuevas leyes y dotarse de nuevas medidas de protección si los usuarios cuelgan información y contenidos que permiten o facilitan la perpetración de delitos.

5. Peligros de las redes sociales

a. Publicación de datos sensibles

i. Vida sexual y amorosa

A través de muchos perfiles se puede conocer la vida amorosa de una persona mediante cambios de estado, mensajes en el muro, fotos, nuevas incorporaciones a la red social... Algunas plataformas como Facebook incitan a incluir información personal al respecto con campos como “Me interesan”, referido a la orientación sexual, “Busco”, o “Situación sentimental”. Publicar la vida amorosa de una persona de forma tan abierta puede incidir en la reputación de una persona. Además de producir situaciones incómodas con otras personas, como pueden ser las antiguas parejas. Últimamente hemos sido testigos de serios problemas debido a esto.

Recientemente apareció una noticia de un asesinato provocado indirectamente por contenidos de Facebook. Un hombre asesinó a su ex mujer y a su hija de cuatro años “cuando se enteró a través de Facebook que mantenía una relación con un antiguo compañero de colegio”⁴⁴. Se trataba de un hombre violento, que sólo necesitó indagar en el perfil de su ex mujer para sufrir un ataque de celos. Antes, cuando una pareja se separaba, la vida privada de la otra persona no se encontraba tan expuesta como ahora. El asesino podría haberse enterado por otros medios, pero nunca quedaría tan claro ni se haría tan público como a través de las redes sociales. Una persona celosa podría conocer todos los detalles de su antigua pareja cómodamente desde su casa a través de un ordenador.

ii. Vida privada

En la cultura de la Web 2.0, el individuo muestra su identidad al mundo a través de fotos de perfil, videos musicales, texto... El uso creciente de Internet en dispositivos móviles permite además la actualización al minuto de la información disponible. Las redes sociales más importantes tienen o tendrán pronto herramientas de localización. Esto permite a los ‘amigos’ compartir información de su localización geográfica en todo momento, y además recibir información de servicios próximos al usuario. Resulta útil o no para el usuario, añadir datos sobre la posición geográfica aumenta sensiblemente la preocupación de los usuarios por su privacidad. Cada vez se incluye información más completa para conformar la identidad virtual, lo cual requiere medidas cada vez más estrictas para proteger a los usuarios.

44

<http://www.telecinco.es/informativos/sociedad/noticia/100018099/Mata+a+su+ex+mujer+y+a+su+hija+de+cuatro+anos+tras+descubrir+en+Facebook+que+tenia+pareja.shtml>

- **Publicación voluntaria de información privada**

Distinguiremos los riesgos relacionados con la diligencia de los usuarios de los inherentes al uso de estas plataformas, que trataremos en el siguiente apartado. Una utilización responsable por parte de los miembros de una red social resulta fundamental para evitar gran cantidad de problemas relacionados con la privacidad.

1. Conductas delictivas

Hemos sido testigos de varios casos de problemas con la justicia en nuestro país debido a publicar contenido probatorio de actos ilegales. Y es que las redes sociales se han convertido en una valiosa herramienta para la policía.

En agosto de 2010, una joven cordobesa fue arrestada tras colgar en Internet fotos suyas cultivando marihuana⁴⁵. Gracias a estas fotos, los agentes de policía pudieron ubicar el lugar y detener a la propietaria por presunto delito contra la salud pública. Este es un caso claro en el que existe un bien superior que proteger (la salud pública), y por tanto prevalece al derecho a la intimidad de la acusada en caso de que hubiera colgado las fotos sólo para su red de amigos y la policía las hubiese interceptado.

Otro caso que causó revuelo fue el de los Guardias Civiles posando en fotos con unas jóvenes durante un botellón y mientras estaban de servicio⁴⁶. Esto no se hubiera conocido públicamente si no fuera porque las jóvenes implicadas decidieron colgar las fotos en Internet, en la red social Tuenti. En las imágenes se aprecia a las jóvenes usando material de la Benemérita. Además una de las jóvenes es menor de edad y se encontraba consumiendo alcohol en presencia de los agentes, sin que éstos tomaran las medidas que requiere la Ley. A raíz de dicho comportamiento, la Comandancia de la Guardia Civil ha expedientado a los dos agentes.

Pero no todo lo que rodea la publicación de la vida privada es negativo. En Nueva York, un joven se ha salvado de ir a la cárcel gracias a Facebook⁴⁷. Rodney Bradford, al que acusaban de cometer un robo, probó su inocencia gracias a una publicación que hizo en la red social en el mismo momento en que lo acusaban de cometer un robo. De este modo se supo que se encontraba lejos del lugar del delito en el momento en que ocurrió. Resulta llamativo que un simple comentario en una red social constituya una cortada lo bastante sólida como para probar la inocencia, a pesar de existir testigos presenciales que situaban a Rodney en la escena del crimen.

⁴⁵ <http://www.elmundo.es/elmundo/2010/08/30/andalucia/1283185848.html>

⁴⁶

<http://www.diariodesevilla.es/article/andalucia/338159/expedientan/dos/guardias/civiles/huelva/por/jugar/con/unas/jovenes/estando/servicio.html>

⁴⁷ <http://edant.clarin.com/diario/2009/11/12/um/m-02039394.htm>

2. Privacidad en el trabajo

Las redes sociales dejan a menudo al descubierto a los empleados. Resulta llamativa la cantidad de despidos motivados por las redes sociales. Por ejemplo, una mujer suiza fue despedida por usar Facebook mientras estaba de baja por enfermedad⁴⁸. La empleada alegó que “no podía trabajar con un ordenador, porque necesitaba estar tumbada en la oscuridad”, y sin embargo actualizaba su estado en Facebook. La empresa ha considerado este acto como un abuso de confianza, lo que ha llevado a la rescisión del contrato.

En otra ocasión, a una trabajadora canadiense se le ha llegado a denegar la pensión por depresión porque su aseguradora encontró en Facebook fotos suyas sonriendo⁴⁹. Las fotos muestran cómo la chica disfruta de la playa y participa en fiestas con las amigas. La aseguradora sostiene que las imágenes demuestran que la joven está totalmente recuperada, y por tanto ha dejado de pagarle, a pesar de que ya no trabaja y asegura seguir estando deprimida.

Además de las mentiras descubiertas a través de las redes sociales, los empleadores también descubren en éstas comentarios de los empleados que los pueden llevar al despido. Una empresa francesa ha despedido a tres empleados por criticar a sus jefes en Facebook⁵⁰. A pesar de tratarse de una conversación privada, un ‘amigo’ pasó una copia de ésta a la dirección de la compañía que los ha despedido. Legalmente no supondría una base suficiente para un despido, ya que, como explican los abogados de los empleados afectados “se trataba de una conversación privada que no ha causado problemas a la compañía”. No obstante los jefes lo han interpretado como “incitación a la rebelión y un menosprecio hacia terceros”.

Por último estudiaremos una medida curiosa implantada en Alemania: la *ley Facebook*, que conlleva la prohibición para el jefe de buscar información personal del empleado. Supone la primera ley para impedir que las empresas utilicen información privada para contratar. Aunque este proyecto refleja la preocupación por parte del gobierno alemán de proteger la privacidad de sus ciudadanos, los juristas afirman que no tiene sentido una ley cuya aplicación resulta imposible de controlar. Los jefes seguirán teniendo accesible la información de sus futuros empleados, y harán uso de ella aunque la Ley se lo prohíba, ya que nadie sabrá que lo han hecho.

3. Vida privada de personajes públicos

Los personajes públicamente conocidos deben tener especial cuidado con la información que divulguen en las redes sociales. Los periodistas pueden utilizarla en su

⁴⁸ <http://www.abc.es/20090424/economia-laboral/despedita-suiza-usar-facebook-200904241749.html>

⁴⁹ http://www.elpais.com/articulo/tecnologia/chica/deprimida/pierde/pension/culpa/Facebook/elpeputec/20091123elpeputec_1/Tes

⁵⁰ http://www.elpais.com/articulo/tecnologia/empresa/francesa/despide/empleados/criticar/jefes/Facebook/elpeputec/20100520elpeputec_6/Tes

contra, o incluso la gente, cuando se trata de una persona que no sea muy apreciada. Es el caso de Eric Besson, ministro de inmigración francés, que publicó la fecha de su boda en Facebook⁵¹. Así, un grupo de casi 1000 fans había amenazado con crear el caos en su boda, lo que le obligó a cambiar la fecha, manteniéndola esta vez en privado.

- **Riesgos inherentes al uso**

El simple hecho de tener un perfil en una red social, independientemente de lo cuidadosos que seamos, nos expone a una serie de riesgos difíciles de controlar. En primer lugar existen **herramientas de análisis social**, de las que hablaremos en el punto 5.3. También hay que tener en cuenta la laguna de las aplicaciones en redes como Facebook, en la que ya no es necesaria la aprobación del usuario.

La configuración por defecto para la privacidad en Facebook es la de “compartir con todos”. Esto significa que, si el usuario no cambia esta opción, compartirá sus datos con **aplicaciones de terceros** para las cuales Facebook no garantiza que sigan las medidas de protección adecuadas. Una vez cedidos los datos personales, resulta muy difícil controlar quién acabará teniéndolos.

Según Artemi Rallo, director de la Agencia Española de Protección de Datos, las redes sociales “no pueden diseñarse pensando en ofrecer por defecto el máximo grado de publicidad de información, sino todo lo contrario”. Defiende que la mayoría de los usuarios utilizan las herramientas que se les ofrecen por defecto, y que por tanto deberían ofrecer el máximo grado de privacidad, para que el usuario que lo desee lo cambie, y el que no lo cambie al menos esté protegido.

Además de las aplicaciones de terceros, es sabido que algunas redes ofrecen sus datos a **organismos oficiales o gubernamentales**. Es lo que ocurre con Twitter, que ha vendido su archivo a la Biblioteca del Congreso de EEUU⁵². Twitter defiende que no se vulnera la inviolabilidad de las comunicaciones dado que los mensajes ya son públicos. No obstante resulta alarmante que una institución de este calibre pueda adquirir información compartida por millones de usuarios.

Por otra parte, conviene mencionar la **falta de protección** existente para los usuarios en cuanto a su información. Como comentamos en el punto 3.5, las redes sociales son el caldo de cultivo perfecto para perpetrar una serie de delitos informáticos. Y la privacidad también puede verse afectada: las escasas medidas de control facilitan el acceso a los hackers a la información personal de los usuarios. Recientemente se publicaron los datos de 100 millones de usuarios de Facebook⁵³. Las redes sociales se están convirtiendo en el lugar más apropiado para el ataque de cierto software malicioso publicitario. Se trata de un fenómeno nuevo y los usuarios, concienciados eso sí, de

⁵¹ <http://www.redessociales.es/2010/09/06/facebook-y-el-cambio-del-dia-de-la-boda-de-eric-besson/>

⁵² <http://www.elmundo.es/elmundo/2010/04/14/navegante/1271273820.html>

⁵³

http://www.elpais.com/articulo/Internet/Publicados/datos/millones/usuarios/Facebook/elpeputec/20100729elpepunet_1/Tes

los emails y las descargas no seguras, no prestan la suficiente atención a la seguridad en las redes sociales.

Para terminar, comentaremos la **vulneración del derecho al olvido** de los miembros de las redes sociales. La justificación jurídica de la permanencia de datos en la red se fundamenta en la veracidad y el interés público de la información. Hay datos que son de interés público, y por tanto deben estar al alcance de todo el mundo. Sin embargo, otros pueden ser ya irrelevantes y causar daños a las personas. Anteriormente, se podía consultar información de hace años en las hemerotecas, pero el acceso a su contenido es mucho más difícil del que ofrece la red.

En lo referente a las redes sociales, el problema radica en que es muy fácil perder el control de la información. Un ejemplo⁵⁴ sería el de un joven de 20 años que cuelga en Tuenti un video bañándose desnudo en una playa de madrugada. Puede resultar divertido en su momento y para su entorno, de modo que este joven elimina el contenido de Tuenti cuando lo considera oportuno. No obstante, el video podría haber pasado ya a otra red, como Youtube, y ser lo bastante público como para encontrarlo en Google a través de su nombre. En el futuro, en un ámbito distinto (como el laboral), la difusión de este video podría tener un impacto muy negativo en la vida diaria de esta persona.

1. Privacidad locacional

En los últimos años hemos sido testigos de una rápida evolución de la utilización de sistemas de localización geográfica en tiempo real en las redes sociales. Primero fue Twitter, luego Tuenti, y próximamente Facebook también ofrecerá Facebook Places, dedicada a este mismo fin. Estos servicios conllevan ventajas claras para el usuario, como poder encontrarse fácilmente con sus amigos, o recibir información útil relativa a su posición. Sin embargo, de este modo queda expuesta la privacidad a otro nivel.

La **privacidad locacional**⁵⁵ (del inglés *locational privacy*) es la seguridad del individuo para poder moverse libremente en el espacio público bajo circunstancias normales, sin que su posición sea grabada sistemáticamente y en secreto para un uso posterior. La publicidad de la posición en sí puede no suponer un problema, pero sí sus implicaciones.

A través del seguimiento geográfico y temporal de una persona, se puede averiguar su sensibilidad política (si acude a una manifestación política determinada), sus relaciones personales (si pasa tiempo en casa de alguien), sus relaciones profesionales (contactos con proveedores), su religión (si frecuenta iglesias, mezquitas o sinagogas), enfermedades (visitas a una clínica especializada en cáncer) y un largo etcétera. Algunas de estas informaciones revelan datos sensibles. Su conocimiento público podría afectar negativamente a la vida de la persona en cuestión.

⁵⁴ <http://www.elmundo.es/elmundo/2010/06/06/navegante/1275818715.html>

⁵⁵ <http://www.eff.org/wp/locational-privacy>

Antes de la existencia de los sistemas de geolocalización, también era posible obtener información de este tipo, pero resultaba un proceso mucho más engorroso. Había que seguir físicamente a la persona, con el riesgo de ser descubierto. Ahora estos datos se pueden obtener de manera permanente, económica, y sin levantar sospechas. Además, algunos organismos los pueden utilizar con fines comerciales o estadísticos.

Las agencias que velan por la protección de los datos personales persiguen que se añadan características de privacidad al diseño de estos nuevos sistemas. Las mismas redes sociales están interesadas, ya que se podrían exponer a cuantiosas multas por parte de distintas entidades, como la AEPD. Sin embargo, se trata de sistemas nuevos, y el desarrollo de técnicas adecuadas para garantizar la privacidad de los usuarios, como puede ser la criptografía, requiere un gran esfuerzo. Habrá que esperar algún tiempo antes de ver perfeccionados los sistemas actuales de geolocalización.

2. Delitos

Algunos delincuentes son conscientes de lo poco cuidadosos que son los usuarios con su información personal. Como es lógico, la gente no revela su información personal a desconocidos de forma física o mediante otros medios más tradicionales, pero a través de sus perfiles en las redes sociales, le brindan acceso a una gran cantidad de información sensible a los delincuentes.

De nada sirve aparentar estar en casa cuando nos vamos de vacaciones si publicamos en una red social que nos hemos ido. Aunque tomemos las medidas típicas como los temporizadores de luz, o pedir a un vecino que recoja un correo, si un ladrón ha visto en nuestra red social un mensaje nuestro, no sólo tendrá la seguridad de que no estamos en casa, sino además cuanto tiempo vamos a estar fuera, permitiéndole así actuar con mayor comodidad⁵⁶. Las entradas en el muro, las actualizaciones de estado o las fotos de nuestro destino son una manera estupenda para los ladrones de obtener información valiosa. Asimismo, mediante los sistemas de localización geográfica pueden saber lo lejos que estamos de casa.

Por otro lado, la información disponible en las redes sociales ha resultado en ocasiones valiosa para los secuestradores⁵⁷, especialmente en países latinoamericanos como México o Brasil. Estos datos les permiten seleccionar a sus víctimas así como acceder más fácilmente a ellas. Con navegar unos minutos, cualquiera puede averiguar el nivel socioeconómico de una persona. La profesión, los vínculos familiares y las fotos de viajes internacionales o de coches y residencias de lujo bastan para conocer de forma aproximada el patrimonio de una persona para saber cuánto exigir en un futuro rescate.

Desde que somos niños, se nos enseña una norma cívica fundamental: no hablar con extraños. Sin embargo, a través de las redes sociales, el ciudadano sirve en bandeja al delincuente todos sus datos personales: ubicación geográfica, nombre completo,

⁵⁶ http://www.elpais.com/articulo/tecnologia/favor/robame/elpeputec/20100218elpeputec_5/Tes

⁵⁷ http://www.clarin.com/policiales/banda-secuestradores-elegia-victimas-sociales_0_309569228.html

números telefónicos, lugar de trabajo, estatus económico... De este modo el secuestrador descubre los lugares que frecuenta una persona, así como la mejor manera de abordarle. Obviamente, los sistemas de localización ayudan todavía más a los delincuentes al ofrecer información en tiempo real del paradero de sus víctimas.

b. Peligros para los menores

Si las redes sociales conllevan riesgos para los adultos, los menores son todavía más vulnerables a otros peligros típicos de su franja de edad. Estos riesgos proceden de prácticas delictivas o dañinas para los jóvenes que ya existían antes de la Web 2.0, como la pornografía infantil, el acoso escolar o la apología de comportamientos perjudiciales para la salud, como la anorexia. Las redes sociales han aportado un nuevo medio para reorganizar las redes de pederastia, continuar el abuso escolar lejos del centro educativo y en general juntar a jóvenes en torno a grupos que en ocasiones pueden causarles daño.

i. Pornografía infantil

En España, el 80% de los adolescentes tiene un perfil en Internet. Es decir, cada vez hay más menores en Internet, los cuales se incorporan cada vez a edades más tempranas. A pesar de que la edad mínima es de 14 años en nuestro país, los menores no dudan en mentir acerca de su edad para formar parte de su red social favorita, en la que también están todos sus amigos, que han accedido de la misma manera. Resulta complicado para las redes controlar esta restricción de edad. Por otro lado, estos jóvenes han pasado de ser víctimas de la pedofilia a ser distribuidores de material de pornografía infantil.

Las denominadas redes de pedofilia, aunque siguen siendo difíciles de erradicar, han sufrido duros golpes policiales, gracias a su labor constante para acabar con esta lacra. Las fuerzas de seguridad del estado poseen potentes herramientas como el programa Híspalis, capaz de rastrear imágenes con contenido pedófilo en la Red, además de agentes encubiertos que han cazado a muchos pederastas.

Debido al auge de las redes sociales entre los menores, los depredadores sexuales encuentran el medio idóneo para acosar a sus víctimas (lo que se conoce como *grooming*). Según indica Jorge Flores, director de Pantallas Amigas, *“el adulto desarrolla la empatía con el niño satisfaciéndole sus necesidades emocionales. El punto de inflexión viene cuando consigue obtener algo de ese menor (un secreto compartido) con lo que poder chantajearle”*. Otra estrategia muy peligrosa es contacto de un menor con un pedófilo que se haga pasar por un menor a través de Internet. Entonces el agresor simula que son “novios” por Internet y consigue fotografías sin ropa. Una vez obtiene esto, el adulto amenazará al niño con que mandará esa foto a todos sus contactos si no hace lo que quiere.

Esta conducta está considerada como delito de inducción de la prostitución de una persona menor, penada con penas de prisión de uno a cuatro años y multa de doce a veinticuatro, o mayores en caso de pertenencia a una organización (artículo 187 del Código Penal). Asimismo, con la reforma de noviembre de 2003 del Código Penal, se contempla por primera vez en España el delito de **posesión de material** pornográfico en cuya elaboración haya sido utilizado a un menor de 18 años (fotografías, vídeos, imágenes reales digitalizadas, archivos electrónicos, etc.). También se introduce el delito de **producción, venta y difusión de pseudo-pornografía**, es decir del material pornográfico donde no se haya utilizado directamente a un menor pero que emplee su imagen o voz alterada o modificada (es lo que se conoce en inglés como 'morphing').

Según un estudio sobre el Nivel de Seguridad de Menores en la Red, uno de cada tres adolescentes contacta con desconocidos a través de la red⁵⁸. Para evitar esta situación, resulta necesario concienciar a los jóvenes para que no se fíen de los desconocidos en la Red, del mismo modo que lo harían en la calle. Además, existe una gran variedad de organismos que luchan por una red más segura para todos. Un ejemplo es 'portaldelmenor.es', que proporciona a los niños un entorno seguro en el que relacionarse, donde se comprueba la identidad del menor individualmente y no se permite la entrada a adultos. Otra iniciativa, Pantallas amigas, promociona el uso seguro y saludable de las nuevas tecnologías en la infancia y la adolescencia.

Las propias redes sociales están tomando conciencia con el asunto. Facebook utiliza un **algoritmo de seguridad** para detectar a los acosadores y los comportamientos considerados como "sospechosos". Entre otros factores el algoritmo tiene en cuenta si el usuario tiene muchos contactos del mismo sexo, como demasiadas mujeres jóvenes; asimismo, vigila si es **rechazado en un gran número de solicitudes de amistad** o envía demasiados mensajes.

Para terminar este apartado, conviene mencionar que se debe tener cuidado a la hora de publicar imágenes de menores. Aunque no se incurra de forma intencionada en pornografía infantil, colgar una foto de familia en la que aparezca una menor en bikini, por ejemplo, podría conllevar consecuencias legales. A pesar de restringir al máximo las opciones de privacidad, se podría considerar una red social como un medio público. Esto estaría perseguido según el artículo 4 de **Ley Orgánica 1/1996 de Protección Jurídica del Menor**, ya que podría "implicar una intromisión ilegítima en su intimidad".

ii. Cyberbullying

De acuerdo con un estudio publicado por el Injuve (Instituto de la Juventud), el 26,6 por ciento de los adolescentes españoles practica o padece cyberbullying.⁵⁹ Para comprender la realidad de esta nueva forma de acoso efectuada a través de las nuevas tecnologías, primero contemplaremos brevemente las características de su variante *offline*: el bullying.

El **bullying**, o acoso escolar, se define como cualquier forma de maltrato psicológico entre escolares, verbal o físico, llevado a cabo, por un grupo o un individuo de forma reiterada contra una víctima que no puede defenderse y a lo largo de un tiempo determinado. Se da mayoritariamente en el aula y patio de los centros escolares. La mayoría de las agresiones son directas, es decir, cara a cara, y se persigue la intimidación de la víctima, implicando un abuso de poder en tanto que es ejercida por un agresor más fuerte.

Desde una perspectiva global, este fenómeno perjudica la calidad de la enseñanza en las escuelas. En cuanto a las víctimas directas, éstas pueden sufrir lesiones

⁵⁸ <http://www.menorenlarede.es>

⁵⁹

<http://www.injuve.migualdad.es/injuve/contenidos.type.action?type=1946804632&menuId=1946804632&mimenu=Gu%EDas%20para%20J%F3venes>

físicas, miedo y ansiedad. Pueden aparecer cuadros depresivos, trastorno de estrés postraumático y síntomas físicos. El acosado vive aterrorizado con la idea de asistir a la escuela y se muestra muy nervioso, triste y solitario en su vida cotidiana. Los daños psicológicos del acosado pueden seguir presentes en la vida adulta del afectado.

Hasta ahora el bullying se limitaba en gran medida al ámbito escolar. Pero con el rápido avance de las tecnologías de la comunicación esto ya no es así. Los jóvenes cada vez se comunican más entre sí y de formas hasta ahora desconocidas para los adultos. Esto les permite continuar el acoso a través de nuevos canales, sin apenas supervisión. Según Bill Belsey, creador del portal bullying.org para ayudar a las víctimas, el ciberbullying “se apoya en el uso de las tecnologías de la información y comunicación para llevar a cabo un comportamiento deliberado, repetitivo y hostil, por parte de un individuo o un grupo, con la intención de hacer daño a los demás”.

En el ámbito de las redes sociales, existen varias herramientas susceptibles de ser empleadas para el acoso. El agresor puede enviar mensajes amenazadores o de odio de forma constante, o insultar a través de la herramienta de chat que algunas poseen. Sin embargo, el mayor daño se produce cuando el agresor emplea canales como el muro, donde **la audiencia puede ser enorme**. Y esta supone una gran diferencia respecto al acoso tradicional. Lo que antes quedaba en el patio de la escuela, ahora lo puede ver todo un instituto. En el muro se pueden colgar imágenes o videos degradantes para el menor abusado, además de insultos y comentarios ofensivos.

Por otra parte, la **naturaleza móvil** de las nuevas tecnologías hace que el acoso sea constante. Los agresores traspasan los límites temporales y físicos que marcaban el acoso en la escuela. El hogar ya no es un lugar de refugio para la víctima, que puede estar pendiente de los contenidos dañinos que se cuelgan acerca de su persona. Incluso los fines de semana o en vacaciones.

Una gran ventaja del ciberbullying para los acosadores es su **anonimato**. Ya no se mofan de la víctima a la cara, como se hacía tradicionalmente. Por tanto pueden sentir menos sentimiento de culpa, e incluso no ser conscientes de las consecuencias de sus actos. Asimismo, tendrán menos probabilidades de ser cogidos, puesto que actúan desde perfiles falsos que posteriormente eliminan, y por tanto cuesta seguirles la pista. De este modo el acoso ya no se limitará necesariamente a alumnos conflictivos con malas relaciones con los profesores, sino que también podría tratarse de alumnos brillantes sin miedo a tener mala fama. Además, como consecuencia del anonimato, los acosadores digitales ya no tienen que ser físicamente más fuerte que sus víctimas, o que estar amparados por un gran número de personas.

Otras características diferenciadoras del ciberacoso serían su carácter **rápido, cómodo e imperecedero**. Ahora resulta muy fácil mantener y expandir el ciberacoso. Basta con copiar y pegar mensajes, mandarlos a grupos muy numerosos de un clic, subir alguna foto o actualizar el estado de cuando en cuando. Además, el contenido digital utilizado se almacena, y hasta que alguien no lo elimine no se pierde. Puede pasar mucho tiempo desde que la víctima denuncia el contenido ofensivo hasta que la red social hace algo al respecto.

Según Willard, existen muchas formas de violencia a través de las nuevas tecnologías. Por un lado están los mensajes vulgares, ofensivos o amenazas.

Seguidamente, tenemos las afirmaciones falsas y crueles en un entorno online. Otra forma muy violenta para la víctima es la suplantación de la persona. De esta forma el acosador puede hacer quedar muy mal al agredido colgando fotos o archivos de texto como si se tratara de la víctima, además de colgar material con información sensible. Por último, los acosadores pueden hacer uso de la exclusión reiterada del individuo, en grupos propios de las redes sociales, por ejemplo.

Según los datos recogidos en la encuesta Generaciones Interactivas⁶⁰, ser usuario de redes sociales incrementa sensiblemente la posibilidad de sufrir acoso a través de Internet. Este hecho es especialmente llamativo entre los 13 y los 16 años, la franja de edad más vinculada a la adolescencia. Los chicos empiezan a sufrir el acoso a una edad más temprana, debido a la precocidad en el uso de las redes sociales. Pero las chicas se declaran víctimas en mayor medida, puesto que utilizan las redes sociales con una mayor intensidad.

⁶⁰ <http://www.generacionesinteractivas.org/>

Tabla 5. Alguien me ha perjudicado a través de Internet (envío de fotos, vídeos, comentarios,...). Por edad: usuarios y no usuarios de redes sociales.

	11	12	13	14	15	16	17	18 años
Usuarios redes	9	7,3	9,3	10	9,4	10,9	6,7	8,7
No usuarios de redes	3,5	5,3	6,5	7,7	7,6	3,7	4,4	11,9

Tabla 6. Alguien me ha perjudicado a través de Internet (envío de fotos, vídeos, comentarios,...). Por género y edad: usuarios y no usuarios de redes sociales.

	11	12	13	14	15	16	17	18 años
Chicos usuarios	10,6	7	8,4	9,5	8,6	7,8	8,5	9,6
Chicas usuarios	6,1	7,6	10,1	10,4	10,2	13,9	4,8	7,8
Chicos no usuarios	2,3	5	5	8,4	8,3	3,3	4,4	5,8
Chicas no usuarias	4,9	5,6	8,6	6,1	6	4,3	4,3	16

Tabla 7. He perjudicado a alguien a través de Internet (envío de fotos, vídeos, comentarios,...).

	11	12	13	14	15	16	17	18 años
Usuarios redes	6,2	4,6	4,8	7,2	7,4	5,9	7	5,6
No usuarios	1,9	2,3	0,9	4,7	5,6	8,8	3,3	5,7

Tabla 8. He utilizado Internet para perjudicar a alguien (envío de fotos, vídeos, comentarios,...). Por género y edad: usuarios y no usuarios de redes sociales.

	11	12	13	14	15	16	17	18 años
Chicos usuarios	9	4,5	5,5	8,9	8,1	8,8	8,7	8,2
Chicas usuarios	1,3	4,7	4,1	5,6	6,6	3,1	5,3	2,5
Chicos no usuarios	2,2	3,2	1,3	5,9	7,6	13,8	4	8,1
Chicas no usuarias	1,5	1,4	0,3	2,1	0,6	0,9	2,3	4,1

iii. Apología de la anorexia y la bulimia

Desde los últimos años han proliferado las páginas en Internet denominadas pro-ana (anorexia) y pro-mía (bulimia). Estas permiten a las jóvenes que sufren trastornos de la alimentación esconder sus problemas alimenticios a padres y médicos. Difunden nuevos “métodos” para perder peso o promueven el uso de fármacos que inducen los vómitos. Estas prácticas son claramente arriesgadas para la salud, a pesar de que estas webs se camuflan como webs de ayuda para la recuperación.

Antes del uso generalizado de las redes sociales, diversas organizaciones denunciaron y lucharon contra estas páginas debido al daño que producen a la sociedad. Sin embargo, a través de redes como Facebook, este daño puede ser mucho mayor. Su componente altamente social permite que la anorexia y la bulimia obtengan características diferenciales en la actualidad. Las jóvenes afectadas sienten que pertenecen a un grupo, el de las jóvenes que comparten la misma enfermedad. Las chicas contactan entre ellas de forma abierta y pública, se motivan mutuamente e intercambian experiencias espeluznantes, sin tener conciencia de su problema. Además la información compartida puede ser muy perjudicial, física y psicológicamente. En un tiempo no tan lejano, el aislamiento y ocultamiento caracterizaban este trastorno. Ahora en las redes sociales incluso se promueven carreras de “perder kilos” entre las jóvenes.

Resulta muy difícil luchar contra estas prácticas. Las distintas plataformas de redes sociales se cubren las espaldas argumentando que no pueden controlarlo todo. Y es que, a efectos legales, en nuestro país poco se puede hacer todavía al respecto. De manera forzada se podría defender que estas páginas suponen un peligro para la salud pública. Aún así, el Defensor del Menor, Arturo Canalda, ha solicitado la reforma del Código Penal incluya como delito la apología de la bulimia y la anorexia que se realiza a través de Internet⁶¹.

⁶¹ <http://www.abc.es/20100616/local-madrid/cursos-anorexia-201006161314.html>

c. Análisis de redes sociales

i. Teoría de redes sociales

El concepto de “red social” existe desde hace más de un siglo para designar a los complejos conjuntos de relaciones entre los miembros de sistemas sociales a todos los niveles, desde interpersonales a internacionales. Durante la segunda mitad del siglo XX, varios académicos han desarrollado teorías para el análisis de redes sociales, que supone todo un paradigma independiente, con sus propias declaraciones matemáticas, métodos, software e investigadores.

El análisis de redes sociales es un método visual y matemático de analizar las relaciones humanas⁶². Se emplea el lenguaje descriptivo de la teoría de grafos como base de su notación. Una red social se define como un conjunto de nodos, que en análisis social representan a los actores de la red, unidos por líneas que representan la relación o relaciones que les unen. Una vez representada la red, se evalúa la posición de los actores, a través de las medidas del concepto de grado (el número de conexiones directas que tiene un nodo), cercanía a otros nodos, y centralización en la red. Los atributos de los individuos son menos importantes que sus relaciones y vínculos con otros actores. Por tanto será de gran relevancia el concepto de **influencia**, definida como la probabilidad asociada a un nodo de transmitir o impedir la transmisión de nuevas ideas o pautas de comportamiento en la red. Se trata por tanto de una técnica clave en la sociología moderna, que tiene aplicación en gran variedad de ámbitos, como son la antropología, biología, ciencias de la información y de la comunicación, económicas, geografía, administración de empresas, psicología social...

ii. Peligro para la privacidad

1. En la política

El problema aparece cuando se utiliza para extraer información personal a nivel de grupo. Estas técnicas pueden ser una herramienta efectiva para la observación de masas, como en el caso del *Total Information Awareness Program* del Departamento de Defensa de los Estados Unidos. Se compone de una serie de programas que comparan numerosos patrones de comportamiento y evalúa si el contexto sugiere que se tratan de terroristas. Se trata de un sistema de conocimiento total de la información. A través de este programa, se han realizado investigaciones detalladas para analizar las redes sociales y así determinar los ciudadanos susceptibles de suponer una amenaza política.

Las consecuencias de un conocimiento tan amplio de las conexiones sociales pueden ser peligrosas. Lo que antes podía suponer un esfuerzo de años, ahora lo pueden hacer potentes programas de software. Por ejemplo⁶³, en los primeros años de la Unión Soviética, los represores rusos ya conocían el valor de las redes sociales. En 1919 un anarquista francés, Victor Serge, fue encargado por el gobierno bolchevique de estudiar

⁶² <http://www.orgnet.com/sna.html>

⁶³ http://lasindias.net/indianopedia/Análisis_de_redes_sociales

los archivos de la policía política zarista. A través de grandes paneles de grafos y cuidadosas anotaciones fruto de años de trabajo, Serge consiguió hacer un seguimiento de quién se carteaba con quién, quién visitaba a quién y quién influía en quién. Este análisis condujo a la encarcelación y a la ejecución de muchas personas contrarias al régimen.

Evidentemente en un estado democrático las consecuencias no serían tan dramáticas, pero a través de las herramientas actuales se puede realizar un análisis mucho más eficaz debido al cual la privacidad de los ciudadanos se encuentra mucho más expuesta. Asimismo, se podrían usar las redes sociales como medio de manipulación. Un análisis puede revelar los nodos más activos y relevantes de la red, hacia los cuales se centraría el esfuerzo para moldear la opinión pública de toda una comunidad. Según el modelo de Michael Chwe⁶⁴, especialista en ciencias políticas, pequeños cambios en grupos determinados o la aparición de nuevos grupos acaban generando cambios de mayorías sociales.

2. Uso poco ético con fines comerciales

Las empresas se han dado cuenta de la influencia que pueden conseguir a través de un análisis conveniente de las redes sociales. Existen herramientas como Facebook Lexicon que permite seguir tendencias entre los usuarios, ya que muestra estadísticas acerca del uso de las palabras en los muros, grupos y eventos en Facebook. En aras de la privacidad, Lexicon no incorpora términos de los mensajes, chat, búsquedas u otra información personal. Del mismo modo, Twist realiza búsquedas sobre las palabras más utilizadas en Twitter. Estas son herramientas públicas y gratuitas al alcance de todo el mundo. De este modo las empresas consiguen estar al día en cuanto a tendencias, opiniones y movimientos de los posibles clientes dentro de la red⁶⁵.

Veamos un ejemplo extraído del blog MarketingProfs⁶⁶. Una empresa de telefonía móvil tiene un cliente que gasta poco, siempre paga tarde, hace un uso abusivo del servicio de atención al cliente y cambia frecuentemente de terminal. A primera vista, parece obvio que le conviene a la compañía deshacerse de un cliente así. Tras un análisis de redes sociales, podríamos ver que no es así. Este cliente podría ser un “nodo” de una compleja red de clientes. Las redes sociales permiten evaluar la importancia de este cliente, especialmente en relación a otros buenos clientes. Tratar de deshacerse de él podría llevarle a hacer publicidad negativa, lo que podría provocar muchas bajas y pérdidas para la empresa. Pero realizar un análisis de sus amigos al mismo tiempo supone una vulneración de la privacidad de esta persona.

La compañía SAS Analytics ofrece una solución de negocio que consiste en extraer valor en tiempo real de la información contenida en las redes sociales y aplicarla a las estrategias de marketing. Esta herramienta puede archivar y analizar más de dos años de conversaciones en medios sociales como Facebook, Twitter o YouTube. Puede recopilar y analizar grandes cantidades de datos, y aporta visión a largo plazo y análisis

⁶⁴ <http://www.chwe.net/michael/socio.pdf>

⁶⁵ http://www.tatum.es/intranet/tatum2003/fotos/pub_fichero375.pdf

⁶⁶ <http://www.mpdailyfix.com/social-network-analysis-hype-or-help/>

avanzado predictivo. Este comportamiento sería claramente ilegal, puesto que no se informa al afectado sobre el tratamiento de sus datos. Y en el caso de que una persona se diera de baja de Facebook, por ejemplo, sus datos no aparecerían en Facebook pero sí en la base de datos de alguna empresa, sin ni siquiera saberlo.

Existe un gran interés en este momento por el desarrollo de herramientas de Software destinadas a extraer información útil (para empresas y gobiernos generalmente) de las redes sociales. Lo cual también genera una gran polémica por parte de los defensores de la privacidad de los usuarios. Un ejemplo llamativo es el proyecto llevado a cabo por dos estudiantes del Instituto Tecnológico de Massachusetts (MIT), que pueden identificar la orientación sexual de una persona en base a la sexualidad y género de los amigos que tiene en las redes sociales. Lo consiguieron analizando los amigos de más de 1.500 perfiles en Facebook de hombres que indicaban explícitamente su condición sexual. Tuvieron en cuenta tres criterios: si eran hombres o mujeres, los intereses y las listas de amigos.

El estudio nos lleva a reflexionar sobre cuánta información sobre uno mismo se puede dar de forma inconsciente por el simple hecho de mostrar en una red social que se es amigo de alguien. La mayoría de las redes sociales permiten navegar por la lista de amigos a todo el mundo, incluso si seleccionamos las opciones de privacidad más restrictivas. Pero vemos que a través del análisis de redes sociales, la propia lista de amigos supone un peligro para la privacidad de los usuarios.

6. Conclusiones

Las redes sociales suponen un tremendo avance respecto a la interacción entre las personas e Internet. La estática Web 1.0, cuya gestión se llevaba a cabo por unos pocos expertos, ha evolucionado mediante nuevos sistemas descentralizados hacia la Web 2.0, dinámica e interactiva. Ahora son los usuarios, en su mayoría sin conocimientos avanzados de informática, los creadores y distribuidores de contenido. Estas plataformas integran todas las herramientas necesarias para llevar una vida social activa a través de un ordenador o incluso del móvil. Somos testigos de un tremendo cambio a la hora de relacionarse, especialmente para los más jóvenes. Muchos pasan tardes enteras en su habitación, relacionándose con sus amigos. Del mismo modo, los adultos pueden reactivar relaciones latentes, como antiguos compañeros de clase, o contactos del entorno laboral.

Las oportunidades que ofrecen estas nuevas herramientas son enormes. En el ámbito empresarial, han aportado un sistema ágil y eficaz de comunicación interna. El nuevo esquema de comunicación motiva a los empleados, lo que contribuye a mejorar el clima laboral. De cara al exterior, es una manera excelente de buscar nuevos empleados para incorporar en la plantilla. Y la gestión efectiva de contactos, sumada a la influencia que permiten ejercer plataformas de este tipo, contribuyen a generar beneficios. El Marketing 2.0 se sirve ampliamente de las redes sociales para que las empresas conozcan mejor a su público objetivo y puedan mostrarse en él. En definitiva, un buen uso de estas redes otorga ventajas importantes frente a aquellas organizaciones que mantienen su modelo de negocio tradicional.

En la política, estos nuevos canales ofrecen algo hasta ahora insólito: bidireccionalidad a gran escala. Los partidos los utilizan para organizarse, comunicarse con el público y animar a la participación. Los pueblos oprimidos se sirven de ellos para oponer resistencia a un gobierno opresor o denunciar al mundo una situación abusiva. Por ello algunos estados los han censurado. Cada vez veremos una presencia mayor de este tipo de medios en las campañas políticas, ya que llegan al público con gran eficacia.

La manera de enseñar también puede verse afectada. La tendencia actual es hacia la enseñanza de tipo B-learning (semi-presencial). Las experiencias piloto realizadas en institutos y universidades con las redes sociales han sido muy positivas. Las redes sociales fomentan el contacto entre el profesor y el alumno. Aumentan la autonomía de los estudiantes y ayudan al profesor a gestionar sus contenidos de forma centralizada, sobre todo con grupos grandes. Existen plataformas que permiten crear redes sociales cerradas con una finalidad concreta. No obstante, a día de hoy sus funcionalidades son insuficientes para la función docente y los profesores a menudo se apoyan en otras herramientas de gestión integral no relacionadas con las redes sociales.

Desgraciadamente las redes sociales también tienen sus debilidades. A través de ellas se pueden vulnerar gran cantidad de derechos, ya que los mecanismos de control existentes no son adecuados para los nuevos medios de comunicación. De aplicarse

todos de forma tajante, resultaría inviable el uso de estas herramientas. A nivel mundial, diversos organismos internacionales han publicado guías y elaborado tratados respecto a la privacidad y a la protección industrial e intelectual. Más tarde, las directivas europeas adaptaron estas ideas, que se plasmaron en las distintas legislaciones nacionales. Sin embargo, éstas siguen siendo muy diferentes entre los distintos estados, por lo que sería deseable un mayor grado de armonización. Además, la directiva de 1995 referente a la protección de datos se está quedando obsoleta y por ello se está redactando una nueva que pronto la derogará.

En España, la Ley Orgánica de Protección de Datos confiere una serie de derechos a los ciudadanos respecto a sus datos personales, y obligaciones a los responsables de ficheros. La Agencia Española de Protección de Datos es la encargada de velar por el cumplimiento de esta ley, y sancionar cuando sea oportuno. Este organismo se ha puesto en contacto reiteradas veces con los representantes de distintas plataformas para que éstas sean más seguras respecto a la privacidad, pero la batalla no ha hecho más que empezar. Algunas redes todavía incumplen la legalidad o podrían mejorar muchos aspectos para proteger al ciudadano lo máximo posible.

En cuanto a la propiedad intelectual, nos enfrentamos a una imposibilidad técnica para dar respuesta a exigencias legales. Los usuarios distribuyen constantemente contenido protegido, sin que sea posible controlarlo debido a la amplitud de las redes. No se permite la reproducción de contenido protegido sin la autorización expresa del autor, pero no tiene sentido prohibir un acto que no se puede controlar. Ni cobrar un canon por los medios de grabación si ya no se graba nada como antes se hacía. Parece evidente que conviene cambiar la legislación de forma que los autores sigan viéndose recompensados por sus creaciones, a la vez que los usuarios puedan distribuir creaciones intelectuales de forma legítima por los nuevos medios.

Los términos de uso han cambiado mucho desde la creación de las redes sociales, en beneficio de los usuarios. Hemos estudiado los casos concretos de Facebook, Tuenti y Twitter. Existe un esfuerzo para proteger a los menores (sobre todo en Tuenti), los contenidos que aporta el usuario se eliminan en cuanto éste se da de baja, y se pueden configurar los parámetros de privacidad. Aún así existen ciertos riesgos. En Facebook hay multitud de aplicaciones a las que cedemos nuestros datos al utilizarlas, y una vez esto ocurre perdemos el control de nuestra información. Aunque tengamos limitada nuestra red a nuestros amigos, nuestra información no está segura.

Muchos usuarios no leen los términos de uso y por tanto están desinformados respecto a los peligros de las redes sociales. La publicación de datos sobre la vida amorosa en las redes ha propiciado venganzas e incluso asesinatos. El contenido de un perfil puede emplearse en contra del usuario, en una investigación policial por ejemplo, si existe un derecho mayor al que proteger. En el mundo laboral, una simple foto de borrachera puede costar el puesto de trabajo a más de uno, o disuadir a un empleador a contratar a una persona.

Cierta información sensible permite la comisión de delitos. A través de las redes sociales un ladrón puede enterarse de la posición de un usuario (por mensajes del

usuario o por las herramientas de localización geográfica) y acudir a robar a su domicilio, estando seguro de que el propietario no volverá. Lo mismo ocurre con los secuestros, ya que se puede determinar el nivel socioeconómico de una persona a través de su perfil, y obtener datos sobre la rutina de los individuos y su posición.

Los menores son especialmente vulnerables a los peligros comentados. La pornografía infantil ha aumentado debido al anonimato y la flexibilidad de este nuevo medio de comunicación. El acoso escolar o bullying ya no se limita al patio del instituto sino que continúa en casa, es lo que se denomina cyberbullying. Asimismo existen páginas susceptibles de dañarles, como las pertenecientes a grupos de extrema derecha, o las que hacen apología de desórdenes como la anorexia y la bulimia. La lucha contra la pornografía infantil es constante desde hace años, y los centros empiezan a tomar conciencia del problema del ciberacoso. Pero todavía no existen leyes específicas contra las páginas que buscan atraer a los menores y que les pueden perjudicar.

El concepto de redes sociales no es ni mucho menos nuevo. Existe una amplia bibliografía al respecto, que incluye técnicas de análisis de este tipo de redes. Se puede extraer mucha información útil de la red de contactos de una persona, sin necesidad de entrar en información personal explícita como las aficiones. Las organizaciones políticas y las empresas podrían emplear herramientas masivas de análisis en las redes sociales para hacer un estudio a gran escala de la población y así propagar mejor unas determinadas ideas o vender mejor un producto en concreto, lo que supone un peligro encubierto para la privacidad de los usuarios.

Las redes sociales son un fenómeno creciente e imparable. Su utilidad es indiscutible, pero no hay que olvidar que el mundo virtual que creamos en ellas sigue siendo real, y por tanto los usuarios deben tomar muchas precauciones a la hora de usarlas. De forma paralela, las instituciones tienen la obligación de publicar nuevas leyes mejor adaptadas a este fenómeno para proteger a los ciudadanos.

REFERENCIAS

1. Estadísticas de Facebook

<http://www.facebook.com/press/info.php?statistics>

(Última consulta: 18-09-2010)

2. El 70% de los adolescentes usa tuenti

<http://www.ethek.com/el-70-de-los-adolescentes-usa-tuenti/>

(Última consulta: 13-04-2010)

3. Los adolescentes y las redes sociales: Del patio del colegio a la Red desde la habitación

<http://revista.consumer.es/web/es/20080601/Internet/72607.php>

(Última consulta: 13-04-2010)

4. La Brecha Digital: Mitos y Realidades, México, 2003

Arturo Serrano, Evelio Martínez, Editorial UABC

www.labrechadigital.org

(Última consulta: 13-04-2010)

5. Los jóvenes y las redes sociales en España

<http://www.facebooknoticias.com/2009/10/02/los-jovenes-y-las-redes-sociales-en-espana/>

(Última consulta: 13-04-2010)

6. El Defensor del Menor tiene un perfil en 'Tuenti' para controlar a sus hijos

<http://www.elmundo.es/elmundo/2010/03/12/madrid/1268412168.html>

(Última consulta: 13-04-2010)

7. ¿Me 'ajuntas'?, versión 2.0.

El País. Edición impresa 01/08/2010, pág. 28-29.

8. El Poder de las Redes.

Manual ilustrado para personas, colectivos y empresas abocados al ciberactivismo.

David de Ugarte.

http://deugarte.com/gomi/el_poder_de_las_redes.pdf

(Última consulta: 09-08-2010)

9. El nuevo ecosistema de la información.

El País Opinión. 9/8/2010.

http://www.elpais.com/articulo/opinion/nuevo/ecosistema/informacion/elpepiopi/20100805/elpepiopi_12/Tes

(Última consulta: 10-08-2010)

10. E-marketing y social media 2010. Universidad Autónoma de Chihuahua

<http://www.slideshare.net/Led146712/emarketing-y-social-media-2010>

(Última consulta: 10-08-2010)

11. Informe del IAB sobre “Redes Sociales en España”

<http://www.iabspain.net/blog/?p=51>

(Última consulta: 10-08-2010)

12. Declaración Universal de los Derechos Humanos

<http://www.un.org/es/documents/udhr/>

(Última consulta: 12-08-2010)

13. Pacto Internacional de Derechos Civiles y Políticos

http://ec.europa.eu/justice/policies/privacy/docs/16-12-1996_en.pdf

(Última consulta: 14-08-2010)

14. Convención sobre los Derechos del Niño

<http://www.margen.org/ninos/derech8b.html>

(Última consulta: 13-08-2010)

15. Agencia de Protección de Datos

<https://www.agpd.es/>

(Última consulta: 13-08-2010)

16. Convenio Europeo para la Protección de los Derechos Humanos y Libertades Fundamentales

http://www.ruidos.org/Normas/Conv_europeo_dchos_hum.htm

(Última consulta: 14-08-2010)

17. Convenio para la protección de individuos con respecto al proceso automático de datos personales

<http://conventions.coe.int/Treaty/en/Treaties/Html/108.htm>

(Última consulta: 14-08-2010)

18. El Exportador Digital (revista Digital del ICEX)

http://www.el-exportador.com/032003/imprimir/portada_articulo.htm

(Última consulta: 16-08-2010)

19. Miles de compradores por Internet venden su alma por no leer la letra pequeña

<http://www.elmundo.es/mundodinero/2010/04/20/economia/1271784338.html>

(Última consulta: 16-08-2010)

20. Términos de uso de Facebook

<http://www.facebook.com/terms.php>

(Última consulta: 18-08-2010)

21. Principios de Facebook

<http://www.facebook.com/principles.php>

(Última consulta: 17-08-2010)

22.Términos de uso de Tuenti

http://www.tuenti.com/#m=Terms&func=view_terms_of_use

(Última consulta: 19-08-2010)

23.Términos de uso de Twitter

<https://twitter.com/tos>

(Última consulta: 19-08-2010)

24.Publicados los datos de 100 millones de usuarios de Facebook

http://www.elpais.com/articulo/Internet/Publicados/datos/millones/usuarios/Facebook/elpeputec/20100729elpepunet_1/Tes

(Última consulta: 23-08-2010)

25.Directorio público de Facebook

<http://www.facebook.com/directory/>

(Última consulta: 23-08-2010)

26.Telegraph. co. uk

<http://www.telegraph.co.uk/technology/twitter/5093060/Twitter-and-Facebook-can-make-you-a-better-worker.html>

(Última consulta: 26/08/2010)

27.Definición de Empowerment – Apuntes de Administración y Dirección de Empresas

http://www.elprisma.com/apuntes/administracion_de_empresas/definiciondeempowerment/

(Última consulta: 26/08/2010)

28.Las empresas miran tu Facebook antes de contratarte

http://www.soitu.es/soitu/2008/01/11/actualidad/1200056997_432019.html

(Última consulta: 26/08/2010)

29.La comunicación empresarial y las redes sociales

<http://www.suite101.net/content/la-comunicacion-empresarial-y-las-redes-sociales-a12039>

(Última consulta: 26/08/2010)

30.33 Million People in the Room

How to Create, Influence, and Run a Successful Business with Social Networking.

Juliette Powell. FT Press 2008.

31.El “Twitterolazo” contra Chávez (ABC.es)

<http://www.abc.es/20100216/medios-redes-web/twitter-chavez-201002162010.html>

(Última consulta: 06/09/2010)

32.Chávez ya tiene cuenta en Twitter (ABC.es)

<http://www.abc.es/20100427/medios-redes-web/chavez-tiene-cuenta-twitter-201004271922.html>

(Última consulta: 06/09/2010)

33.China bloquea YouTube y ‘The Guardian’ tras los disturbios en el Tíbet

<http://www.elmundo.es/navegante/2008/03/17/tecnologia/1205745625.html>

(Última consulta: 07/09/2010)

34.China bloquea Twitter y Hotmail en vísperas del aniversario de Tiananmen
<http://www.elmundo.es/elmundo/2009/06/02/internacional/1243963540.html>
(Última consulta: 07/09/2010)

35. China bloquea también Facebook
<http://www.elmundo.es/elmundo/2009/07/08/navegante/1247035807.html>
(Última consulta: 07/09/2010)

36.Informe de Simon Wiesenthal (mayo 2009)
<http://www.wiesenthal.com/site/apps/nlnet/content2.aspx?c=lsKWlbpJLnF&b=4441467&ct=6994349>
(Última consulta: 07/09/2010)

37.Facebook expulsa de su comunidad a varios grupos neonazis
http://www.elpais.com/articulo/Internet/Facebook/expulsa/comunidad/varios/grupos/neonazis/elpepunset/20081117elpepunset_1/Tes
(Última consulta: 07/09/2010)

38.Más de mil personas dicen 'Basta ya' a la corrupción en una manifestación en Palma
<http://www.elmundo.es/elmundo/2009/12/12/baleares/1260622017.html>
(Última consulta: 07/09/2010)

39.Israel me ha mandado un Tweet
<http://guerreando.wordpress.com/2010/06/07/israel-me-ha-mandado-un-tweet-el-poder-de-las-redes-sociales/>
(Última consulta: 07/09/2010)

40.Las redes sociales, fundamentales para el triunfo de Obama
http://www.tendencias21.net/Las-redes-sociales,-fundamentales-para-el-triunfo-de-Obama_a2717.html
(Última consulta: 08/09/2010)

41.Las redes sociales aplicadas a la práctica docente
Juan José de Haro. Revista DIM: Didáctica, Innovación y Multimedia, Nº. 13, 2009

42.Las redes sociales en educación
<http://jjdeharo.blogspot.com/2008/11/la-redes-sociales-en-educacin.html>
(Última consulta: 10/09/2010)

43.WEB 2.0. Un nuevo entorno de aprendizaje en la Red
Francisco José Ruiz Rey. Revista DIM: Didáctica, Innovación y Multimedia, Nº. 13, 2009

44.Mata a su mujer y a su hija tras descubrir en Facebook que tenía pareja
<http://www.telecinco.es/informativos/sociedad/noticia/100018099/Mata+a+su+ex+mujer+y+a+su+hija+de+cuatro+anos+tras+descubrir+en+Facebook+que+tenia+pareja.shtml>
(Última consulta: 11/09/2010)

45.Arrestada tras colgar en Internet fotos suyas cultivando marihuana
<http://www.elmundo.es/elmundo/2010/08/30/andalucia/1283185848.html>
(Última consulta: 15/09/2010)

46.Expedientan a dos guardias civiles por ‘jugar’ con unas jóvenes estando de servicio

<http://www.diariodesevilla.es/article/andalucia/338159/expedientan/dos/guardias/civiles/huelva/por/jugar/con/unas/jovenes/estando/servicio.html>

(Última consulta: 15/09/2010)

47.Un joven se salva de la cárcel gracias a un mensaje en Facebook

<http://edant.clarin.com/diario/2009/11/12/um/m-02039394.htm>

(Última consulta: 15/09/2010)

48.Despedida una suiza por usar Facebook mientras estaba de baja por enfermedad

<http://www.abc.es/20090424/economia-laboral/despedita-suiza-usar-facebook-200904241749.html>

(Última consulta: 15/09/2010)

49.Una chica deprimida pierde la pensión por culpa de Facebook

http://www.elpais.com/articulo/tecnologia/chica/deprimida/pierde/pension/culpa/Facebook/elpeputec/20091123elpeputec_1/Tes

(Última consulta: 15/09/2010)

50.Una empresa francesa despide a tres empleador por criticar a los jefes en Facebook

http://www.elpais.com/articulo/tecnologia/empresa/francesa/despide/empleados/criticar/jefes/Facebook/elpeputec/20100520elpeputec_6/Tes

(Última consulta: 15/09/2010)

51.Facebook y el cambio del día de la boda de Eric Besson

<http://www.redessociales.es/2010/09/06/facebook-y-el-cambio-del-dia-de-la-boda-de-eric-besson>

(Última consulta: 15/09/2010)

52.La Biblioteca del Congreso de EEUU adquiere el archivo de Twitter

<http://www.elmundo.es/elmundo/2010/04/14/navegante/1271273820.html>

(Última consulta: 15/09/2010)

53.Publicados los datos de 100 millones de usuarios de Facebook

http://www.elpais.com/articulo/Internet/Publicados/datos/millones/usuarios/Facebook/elpeputec/20100729elpepune_1/Tes

(Última consulta: 15/09/2010)

54.El derecho al olvido o desaparecer del ciberespacio

<http://www.elmundo.es/elmundo/2010/06/06/navegante/1275818715.html>

(Última consulta: 15/09/2010)

55.On Locational Privacy, and How to Avoid Losing it Forever

<http://www.eff.org/wp/locational-privacy>

(Última consulta: 15/09/2010)

56.Por favor, róbame

http://www.elpais.com/articulo/tecnologia/favor/robame/elpeputec/20100218elpeputec_5/Tes

(Última consulta: 15/09/2010)

57.Una banda de secuestradores elegía a sus víctimas por redes sociales

http://www.clarin.com/policiales/banda-secuestradores-elegia-victimas-sociales_0_309569228.html

(Última consulta: 15/09/2010)

58.Menor en la red

<http://www.menorenared.es/>

(Última consulta: 15/09/2010)

59.Injuve

<http://www.injuve.migualdad.es/injuve/contenidos.type.action?type=1946804632&menuId=1946804632&mimenu=Gu%EDas%20para%20J%F3venes>

(Última consulta: 16/09/2010)

60.Generaciones interactivas

<http://www.generacionesinteractivas.org/>

(Última consulta: 16/09/2010)

61.La Comunidad imparte cursos contra la anorexia y la bulimia

<http://www.abc.es/20100616/local-madrid/cursos-anorexia-201006161314.html>

(Última consulta: 16/09/2010)

62.Social Network Analysis

<http://www.orgnet.com/sna.html>

(Última consulta: 18/09/2010)

63.Análisis de redes sociales

http://lasindias.net/indianopedia/Análisis_de_redes_sociales

(Última consulta: 18/09/2010)

64.Structure and Strategy in Collective Action

<http://www.chwe.net/michael/socio.pdf>

(Última consulta: 18/09/2010)

65.Tatum

http://www.tatum.es/intranet/tatum2003/fotos/pub_fichero375.pdf

(Última consulta: 18/09/2010)

66.Social Network Analysis: Hype or Help?

<http://www.mpdailyfix.com/social-network-analysis-hype-or-help/>

(Última consulta: 18/09/2010)

Otro material consultado

Social Network Sites: Definition, History, and Scholarship

Danah M. Boyd, Nicole B. Ellison. Michigan State University, 2007.

All a Twitter: A Personal and Professional Guide to Social Networking with Twitter

Tee Morris Indianapolis, Ind.: Que, 2009.

Facebook Cookbook

Jay Goldman Edición 1st ed. Sebastopol, California, O'Reilly, 2009.

The Wealth of Networks.

Yochai Benkler. Yale University Press.

Designing for the social web

Joshua Porter. New Riders, 2008.

I Jornadas Universitarias Derecho y Sociedad

Colegio Mayor Universitario de la Alameda. Abril 2010.

Deontología y Aspectos Legales de la Informática: Cuestiones éticas, jurídicas y técnicas básicas

María del Rosario de Miguel Molina, Juan Vicente Oltra Gutiérrez
Universidad Politécnica de Valencia. Servicio de Publicaciones, 2007.

Redes Sociales Y Efectos Jurídicos

<http://www.slideshare.net/lidiasanizo5/redes-sociales-y-efectos-juridicos-1995902>

(Última consulta: 13/04/2010)

Enterprise Web 2.0 Fundamentals

Krishna Sankar, Susan A. Bouchard. Cisco, 2009.

Web 2.0.

Regulación legal: Acciones de Marketing y redes sociales.
Riestra Abogados. Interactive Advertising Bureau. Junio 2009.